

atp | journal

7/2019

PRIEMYSELNÁ AUTOMATIZÁCIA A INFORMATIKA

NEPODCEŇUJTE ÚTOKY

INTEGROVANÉ STROJOVÉ VIDENIE
Viac ako kamery

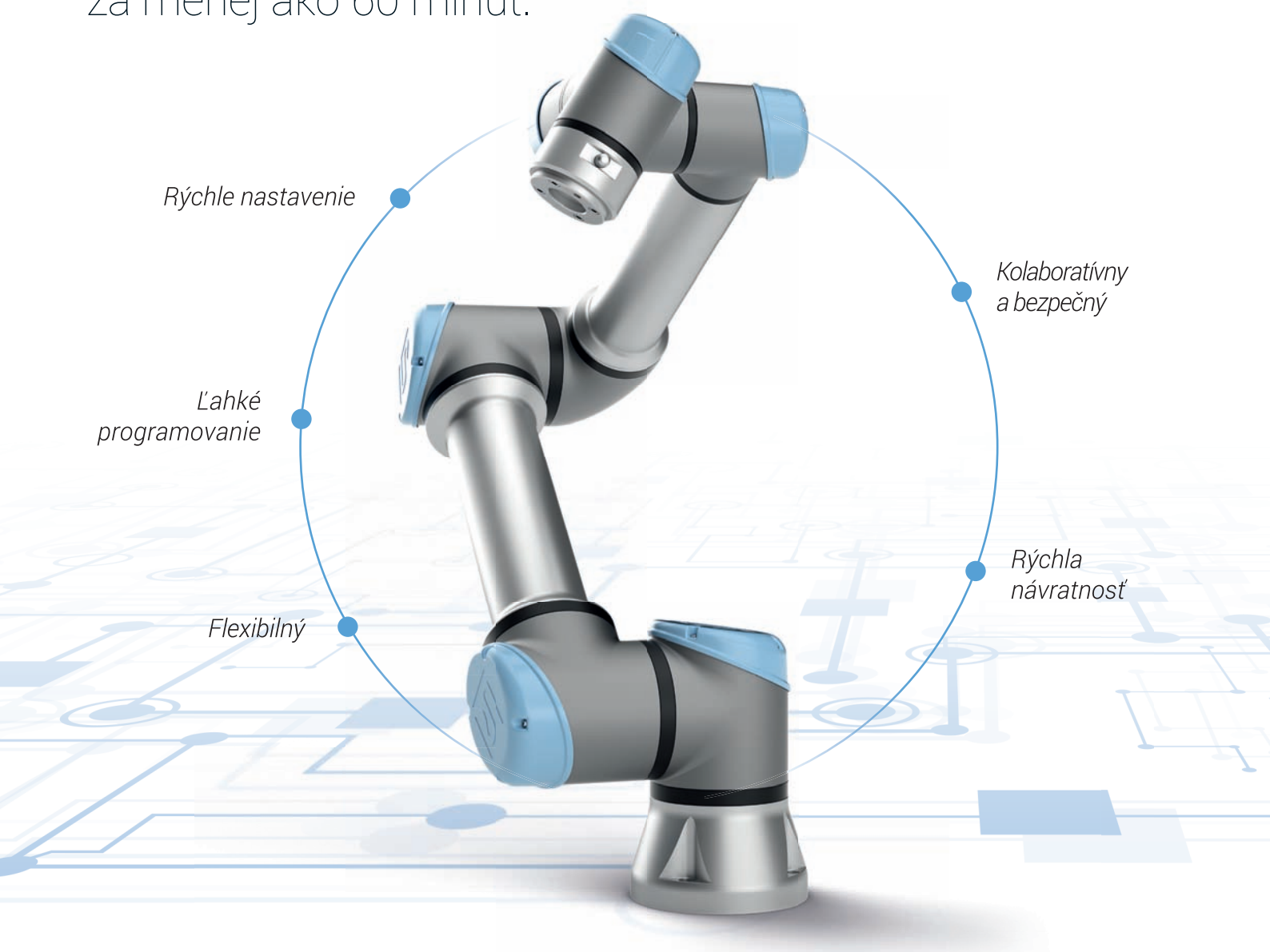


PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP



RÝCHLA CESTA K ÚSPECHU.

Coboty radu e-Series rozbalíte, upevníte a nastavíte za menej ako 60 minút.



Rad e-Series skracuje čas nastavenia robota z dňov na minúty. S pokročilými technológiami a funkciami, ktoré umožňujú rýchle nastavenie, bezproblémovú

integráciu a ľahké programovanie, mení e-Series spôsob, akým budú podniky automatizovať svoje prevádzky. Zefektívnete svoje podnikanie s e-Series.

Viac informácií o e-Series nájdete
na universal-robots.com/cs/e-series/

 **UNIVERSAL ROBOTS**

N a š a c e s t a v e d i e k v á m



Sme súčasťou energetického cievného systému Európy. Plníme strategickú, pre organizmus hospodárstva Slovenskej republiky životne dôležitú funkciu. Naším poslaním je vytvoriť podmienky na spoľahlivú dodávku elektriny všade tam, kde je nevyhnutná pre každodenný život a chod krajiny.



Slovenská elektrizačná prenosová sústava, a.s.
Mlynské nivy 59/A, 824 84 Bratislava 26, Slovensko
www.sepsas.sk



INTERVIEW

4 Nepodceňujte útoky

APLIKÁCIE

- 8 Sledovanie výroby pomocou RFID
- 12 Decentralizované riadenie s odolným PLC
- 15 Najvyššia presnosť pri plnení viskózneho bitúmenu
- 16 Kolaboratívny robot pomohol urýchliť a zefektívniť výrobu

PRIEMYSELNÝ SOFTVÉR

- 18 EPLAN Pro Panel a Rittal Perforex – víťazná kombinácia!
- 19 OBO Construct
- 20 Systém riadenia priemyselnej kybernetickej bezpečnosti
- 22 Riešenia kybernetickej bezpečnosti end-to-end pre automatizáciu

RIADIACA A REGULAČNÁ TECHNIKA

- 24 Voľne programovateľný izbový regulátor SBC pre pružné a individuálne aplikácie
- 25 Phoenix Contact predstavuje programovateľný systém logických relé PLC logic

UMELÁ INTELIGENCIA

- 26 Zmeňme výrobu z automatizovanej na autonómnu
- 45 Umelá inteligencia pracovné miesta tvorí, nelikviduje
- 46 Metódy strojového učenia v službách kybernetickej bezpečnosti CAV (1)
- 50 Smart/Intelligent edge – poskytovatelia platforiem cloud a edge

PRIEMYSELNÉ PC

- 28 Nová generácia Beckhoff IPC a UPS

ROBOTIKA

- 30 Prudký rast trhu kolaboratívnych robotov
- 32 YASKAWA „všetko v jednom“: robotika a riadenie pohybu

PREVÁDZKOVÉ MERACIE PRÍSTROJE

- 33 Kalibrácia HART prevodníkov tlaku
- 34 Kalibračná neistota pre nematematickov

PRIEMYSELNÁ KOMUNIKÁCIA

- 38 Open Source IIoT Gateway RevPi Connect s väčšou pamäťou

ZDROJE, UPS

- 39 „Čo najneskôr, ako sa dá, avšak hneď, ako je potrebné.“
- 40 Správny prístup k výberu a návrhu napájania

PRIEMYSEL 4.0

- 42 Digitálny kalibračný certifikát (2)

ODBOROVÉ ORGANIZÁCIE

- 53 Elektrotechnické STN

VZDELÁVANIE, LITERATÚRA

- 54 Odborná literatúra, publikácie

PARTNERSKÉ ORGANIZÁCIE ATP JOURNAL



Kybernetická bezpečnosť naberá na dôležitosti

Človek zostáva pre priemyselné riadiace systémy a súvisiace siete najväčšou hrozbou z hľadiska ich bezpečnosti. Vyplynulo to z prieskumu inštitútu SANS zameraného na lepšie pochopenie kybernetických bezpečnostných rizík týkajúcich sa prevádzkových technológií. Problémom však stále zostáva identifikácia pripojených technických prostriedkov a získanie prístupu do zariadení, sietí a integrity riadiacich systémov. Dalším rizikom je aj stále rastúci prechod do cloudových systémov.

A čo odporúčajú odborníci? Pravidelne aktualizovať operačné systémy, aplikačný softvér na systémoch, ktoré sú súčasťou priemyselných sietí. Nasadzovať bezpečnostné záplaty do PLC, RTU a sieťových zariadení v rámci sietí priemyselných riadiacich systémov. Obmedziť sieťovú premávku na portoch a protokoloch používaných na okrajových smerovačoch a vnútri prevádzkových sietí. Audítovať riadenie prístupu pre prvky priemyselných riadiacich systémov v rámci priemyselných sietí a na ich okrajoch. Zabezpečiť, aby boli bezpečnostné systémy stále aktualizované a systémy určené na ochranu pred útokmi správne nasadené. A je toho ešte podstatne viac. O tom, že téma kybernetickej bezpečnosti naberá na obrátkach, svedčí nielen rastúci počet odborných podujatí venujúcich sa tejto téme, ale aj rastúce množstvo zrealizovaných útokov na priemyselné prevádzky. Aj preto prinášame v tomto čísle viacero exkluzívnych príspevkov, ktoré problematiku kybernetickej bezpečnosti rozoberajú z rôznych uhlov pohľadu – od etických hackerov cez tvorcov bezpečnostných riešení až po inžiniersku spoločnosť a jej skúsenosti s nasadzovaním bezpečnostného systému v slovenskom priemyselnom podniku.



Anton Gérer
šéfredaktor

NEPODCEŇUJTE ÚTOKY

Čoraz viac prepojení medzi zariadeniami a technológiami navzájom, čoraz viac prepojení na vonkajší svet. To je realita dnešného moderného priemyselného podniku. S ňou však prichádzajú aj rôzne výzvy. Tie sa týkajú aj bezpečnosti údajov a ich ochrany pred zneužitím neoprávnenými osobami či zasahovaním do činnosti výrobných prevádzok. Ako sa proti tomu brániť a ako sa dá riešiť problematika toľko medializovanej kybernetickej bezpečnosti? Aj o týchto témach sme sa porozprávali s Tomášom Zaťkom, výkonným riaditeľom spoločnosti Citadelo, ktorej mottom je „Hackeri na vašej strane“.

Prečo by sa priemyselné podniky mali vôbec venovať otázkam kybernetickej bezpečnosti?

Ak sa jej priemyselné podniky nebudú venovať, tak môžu veľmi ľahko naraziť na problémy, ktoré budú viesť k nemalým finančným stratám. V horšom prípade to môže viesť až k dramatickému ohrozeniu výrobných technológií, životného prostredia či fyzického zdravia pracovníkov. Avšak vo väčšine prípadov kybernetických hrozieb ide o ekonomické problémy.

Predstava o kybernetickej bezpečnosti sa často spája s IT systémami na vrchných úrovniach podniku. Avšak dnes je situácia iná v tom, že podniky majú už často prepojené siete na úrovni IT a výrobných prevádzok (OT). Treba teda vnímať kybernetickú bezpečnosť takto komplexne?

Samozrejme, dnes sa už nepripájajú do siete len kancelárske PC, ale aj výrobné a technologické zariadenia na úrovni prevádzky. Takže aj prístup k riešeniu kybernetickej bezpečnosti by mal tieto realie zohľadniť.

Aký je aktuálny stav v oblasti riešenia kybernetickej bezpečnosti v priemyselných podnikoch z hľadiska noriem a legislatívy?

Doteraz sme mali vždy možnosť oprieť sa o nejaké normy či skúsenosti zo zahraničia. Je škoda, že sa o tejto téme začalo na Slovensku hovoriť vo veľkom až teraz, keď bol schválený zákon č. 69/2019 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Riešenie kybernetickej bezpečnosti by pre firmy malo byť zaujímavé bez ohľadu na to, či je to dané existenciou nejakého zákona. Viaceré firmy už v predchádzajúcom období na základe existujúcich noriem, osvedčených postupov a bezpečnostných opatrení spracovali a uviedli do života programy kybernetickej bezpečnosti, preto schválenie kybernetického zákona v rámci legislatívy SR pre nich veľa zmien v zásade neprináša. Rozdiel medzi Slovenskom a zahraničím je však v tom, že veľa firiem túto problematiku doteraz pokrytú nemalo, takže zákon na ne efektívne zatlačil, aby to riešiť začali. Pokiaľ niekto doteraz nemal skúsenosť s kybernetickými prienikmi do svojej infraštruktúry, môže sa mu riešenie tejto problematiky javiť ako niečo veľmi vzdialené. Argumentácia „nás sa to netýka“ je často prvým krokom k zabrzdzeniu výdavkov do oblasti kybernetickej bezpečnosti. Je zjavné, že firmy, ktoré už s kybernetickým útokom mali skúsenosť, vedľa rýchlo nájsť prostriedky na riešenie tejto problematiky. Lenže keď sa už útok uskutoční, rozpočet potrebný na riešenie problému je často podstatne vyšší v porovnaní s rozpočtom v preventívnej fáze.

Aké sú základné myšlienky, ktoré by si firmy so snahou riešiť kybernetickú bezpečnosť mali v existujúcom zákone všimnúť?

Zákon definuje, koho sa týka. Ak môj podnik spadá do pôsobnosti tohto zákona, treba si podrobne naštudovať celý zákon. Ja by som upriamil pozornosť najmä na bezpečnostné opatrenia definované v §20. Sú rozdelené do určitých kategórií z hľadiska technických prostriedkov, procesných postupov a pod. Ak už napríklad podnik riešil otázku kybernetickej bezpečnosti podľa normy ISO/IEC 270002, príp. inej normy ohľadom priemyselnej kybernetickej bezpečnosti, veľa vecí má vyriešených. Zákon pokrýva aj témy, ako sú vzťahy s dodávateľmi, čo je mimoriadne dôležité, pretože útoky často prichádzajú práve cez tieto tretie strany. Ak je táto implementácia častí kybernetickej bezpečnosti v podniku už vyriešená, ďalšia oblasť, ktorú zákon pokrýva, je uvedená v §29 a týka sa auditu kybernetickej bezpečnosti. Ten je najlepšie zrealizovať prostredníctvom nezávislého subjektu s danou kompetenciou, ktorý posúdi, v akom stave sa celé riešenie bezpečnosti nachádza. Zákon ďalej upravuje povinnú súčinnosť so štátom. Ak je môj podnik prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby, podnik je povinný hlásiť incidenty štátnej jednotke na riešenie kybernetických incidentov. Pre stranu štátu zákon definuje postavenie, úlohy a povinnosti jednotlivých štátnych inštitúcií.



Je rozdiel medzi vedením a intenzitou kybernetických hrozieb na úrovni podnikových IT a technológií nachádzajúcich sa na úrovni výrobných prevádzky (OT)?

Rozdiely tam určite sú. Odborníci na rôznych úrovniach podniku vnímajú hrozby rôzne, na základe tých priorit, ktoré majú v rámci svojho pracovného zaradenia. Z technologického hľadiska sa IT a OT k sebe čoraz viac približujú a sú čoraz viac prepojené. Kým pred dvadsiatimi rokmi svet počítačov a počítačových sietí a svet výrobných prevádzok a tam nasadených technológií bol dosť rozdielny, dnes sa aj v OT používajú čoraz viac tie isté technológie a protokoly ako v IT. Táto skutočnosť zjednodušuje útočníkom prienik do infraštruktúry podniku, nakoľko menšia modifikácia nástrojov a postupov na prienik z oblasti IT bude účinná aj v OT. Z pohľadu spôsobu zabezpečenia IT a OT je to však výrazne odlišné. Ak mojím primárnym cieľom v rámci bezpečnosti IT je, aby nedošlo k úniku údajov, tak v rámci OT je kľúčovou metrikou dostupnosť systémov a zariadení. Toto celé ovplyvňuje spôsob nasadzovania a testovania systémov zabezpečenia. Penetračné testy, čiže simulované hackerské útoky v rámci OT, sú výrazne komplikovanejšie ako vo svete IT. Pokiaľ ide o útok, kde je snahou odhaliť slabiny niekedy vedúce až k výpadku IT, tak v OT to v živej prevádzke nie je možné. V takomto prípade treba využiť nejaké klony reálnej technológie.

Byť či byť pripojený do internetu na úrovni výrobných prevádzky – to je otázka!

Otázka vyzerá jednoducho, ale odpoveď až taká jednoduchá nie je. Veľmi ľahko by sa dalo povedať, že samozrejme, na úrovni prevádzky je najlepšie byť pripojený do internetu. Potom nás nikto nehackne. Ako potom chceme využiť všetky prínosy spojené s pripojením do globálnej siete? Pripojenie na internet má väčšinou nejaké dobré biznis dôvody. Určite si však treba dávať pozor na to, čo a akým spôsobom pripojíme, v akom režime či s akými obmedzeniami. Veľmi často sa ukazujú nepríjemné prípady, keď bol nejaký systém, resp. jeho pripojenie na internet navrhnutý zdanlivo neškodným spôsobom, napr. že cez internet budem iba jedným smerom načítavať nejaké hodnoty (klasická telemetria). Často sa však ukážu programové chyby, resp. chyby spôsobené rozdielom v tom, ako sme to riešenie plánovali realizovať a ako sme ho potom skutočne zrealizovali. Tieto chyby môžu vyústiť do toho, že viem z daného systému nielen čítať údaje, ale zrazu mám ako neautorizovaná osoba aj možnosť niečo meniť či riadiť v danej prevádzke. Každý, kto sa snaží odpovedať na uvedenú otázku, by sa mal veľmi dobre zamyslieť a nepodceňiť to.

Kde sú slabiny priemyselných riadiacich systémov z hľadiska kybernetickej bezpečnosti?

Na túto otázku opäť nemožno odpovedať jednoducho už aj z toho dôvodu, že slabín priemyselných riadiacich systémov je viacero. Spomením len pár príkladov z našej praxe, ktoré však zďaleka nepokrývajú celú paletu. Počas tohtoročného Medzinárodného strojárského veľtrhu v Nitre sme prezentovali ukážku toho, ako sa dá zaútočiť na kompletne vzdušne oddelený systém bez fyzického pripojenia k internetu. Ukázali sme sériu krokov, pomocou ktorých sa dá doručiť útočný kód priamo do prevádzky oddelenej od zvyšku sveta. Prípad asi najznámejšieho priemyselného kybernetického útoku Stuxnet je tomu podobný. Iný typ útokov má pôvod v tom, že na zariadenia, ktoré sú morálne zastarané, sa niekto snaží pripojiť nové elektronické prvky, ktoré majú možnosť pripojenia na internet. V rámci našej činnosti sme robili testovanie istého radu priemyselného riadiaceho systému, ktorý pracuje úplne bezproblémovo. Avšak v rámci novej verzie tohto systému výrobca pridal možnosť prístupu aj cez internet. Z našej analýzy vyplynulo, že pre samotného výrobcu zariadenia bolo ťažké na hardvér, ktorý má bez zásadnejších zmien už okolo dvadsať rokov, implementovať určité moderné technológie, aby sa prostredníctvom tohto riadiaceho systému dalo robiť vzdialené a navyše bezpečné riadenie. Na uvedený hardvér neexistovali dostatočne moderné softvérové knižnice, a tak bol výrobca nútený použiť staršie. Staré kusy softvéru obsahovali chyby, ktoré sú v novších systémoch dávno ošetrované. Na otestovanie sme v rámci našich penetračných testov museli siahnuť po hackerských metódach pred dvadsiatimi rokmi, ktoré sa už dnes



takmer nepoužívajú. Často tiež vidíme, že zákazníci majú optimistické predstavy o tom, ako sú ich jednotlivé podsiete oddelené, ale veľké množstvo existujúcich výnimiek je v realite od tej predstavy oddelenia sietí veľmi ďaleko.

Znamená to, že v prvom rade by si mali ujasniť problematiku kybernetickej bezpečnosti svojich priemyselných riadiacich systémov ich výrobcovia?

Áno aj, pretože to je len jedna časť príbehu. Môže sa samozrejme stať, že samotný výrobca nemá otázku bezpečnosti úplne doriešenú, druhá vec je, ako tento riadiaci systém alebo nejaký komponent integrujem do zvyšku technológie, a do tretice je dôležité aj to, ako sa o tento komponent priebežne starám. Dodávateľ mi môže dodať z hľadiska bezpečnosti dobrý komponent, ale následne ho môžem integrovať takým spôsobom, že otvorím cestu na hackerský útok. Problém môže byť napríklad v tom, že ponechám na zariadení prednastavené heslá od výroby. Ďalší problém je, že často sa požaduje segregácia sietí a tá, ako sme mali možnosť vidieť v reálnej praxi, sa deje často len na úrovni sietí VLAN, ktoré boli aj tak pozapájané do jedného fyzického zariadenia. Videli sme prípad, keď sa zálohy konfigurácie sieťového zariadenia ukladali na zálohovací server. Nám sa podarilo preniknúť útokom na tento server, z ktorého sme sa následne vedeli dostať na sieťové zariadenie a urobiť si nové pripojenia do jednotlivých sietí VLAN. Častou chybou je, že spoločnosti buď nemajú nasadený monitoring útokov a prienikov, alebo ak ho aj majú nasadený, nikto na oznamy a upozornenia z neho nereaguje.

Dá sa vôbec pri firme, ktorá nemá nasadený monitoring bezpečnosti, zistiť príčina, resp. slabé miesto, kadiaľ útočníci prenikli?

Máme skúsenosť z auditu vo firme, kde prišlo k hackerskému útoku. Vzhľadom na to, že firma nemala nasadený monitoring prienikov



svojich systémov, bolo veľmi ťažké identifikovať, kadiaľ útok prebehol. Logové záznamy, ktoré by mohli niečo napovedať, sa premazávali na týždenné báze. Zákazník si útok, resp. jeho dôsledky všimol podstatne neskôr. Sami sme následne identifikovali štyri možné cesty, kadiaľ mohol byť útok vedený, ale s istotou sme nevedeli posúdiť, ktorá to v skutočnosti bola. Ďalší zákazník síce mal nainštalovaný systém monitorovania, ktorý im aj včas hlásil prebiehajúci útok, ale nikto na to nereagoval. A prečo? Lebo zodpovednosť vo firme bola nastavená tak, že človek, ktorý mal vo svojej kompetencii na to reagovať, mal okrem toho na starosti mnoho iných vecí, ktoré ho zamestnávali natoľko, že na reagovanie na prebiehajúci útok nezvyšil čas. Ďalšou chybou je, keď zákazník optimisticky nasadí rozsiahlu paletu obranných mechanizmov a systémov a nechá si to overiť penetračnými testami. Je jednoduché vymyslieť systém, ktorý ja sám neprekonám, ale ani v reálnej prevádzke sa nechránime sami pred sebou, ale hrozbami zvonku. Ak má zákazník nainštalovaný systém riadenia prevádzkovej bezpečnosti (Security Operation Center) a má na to aj vyčlenených ľudí, je dobré raz za čas spraviť test celého systému a zistiť, či bezpečnostné prvky aj monitoring naozaj spoľahlivo fungujú.

Aké sú najčastejšie slabé miesta priemyselných podnikov, ktoré hackeri zvyknú zneužiť na svoje útoky?

Odpoveď na túto otázku sa mení v čase. Iná by bola pred piatimi rokmi, iná dnes a iná bude pravdepodobne o päť rokov. V súčasnosti sú také dve hlavné cesty, kadiaľ sa útočníci dostávajú ku kritickým zariadeniam a technológiám v priemyselných podnikoch. Sú to už spomínané tretie strany zaradené v rámci dodávateľských reťazcov alebo cez interných zamestnancov. V druhom prípade môže vzniknúť dojem zo strany vedenia spoločnosti, že si chovajú „hady na prsiach“, ale to tak vôbec nemusí byť. Často sú totiž interní zamestnanci, ktorí sa stanú vstupnou bránou do podniku, sami zneužití bez toho, aby o tom vedeli. Jednou z tých starých, ale stále fungujúcich metód, sú phishingové emaily. Inak slovo phishing je odvodené od slova fishing a v prenesenom význame znamená tiež chytanie obete na návnadu. Zamestnanec dostane e-mail od falošného odosielateľa, v ktorom je priložený nejaký dokument, čo môže byť špeciálne upravený Word alebo PDF. Po jeho otvorení sa vykoná nejaký program, ktorý využije nechránený prehliadač PDF dokumentov, v ktorom ešte nebola nainštalovaná najnovšia záplata. Tým sa vytvorí vstupná brána do zvyšku siete a následne má útočník pomerne dosť veľa času na aktiváciu svojej činnosti. Keď je útok dokonaný, často sa pri spätnej analýze celého incidentu zistí, že prienik sa udial niekedy mesiac pred samotným zaregistrovaním záškodnej

činnosti. Útočník za ten čas postupne prechádzal rôznymi stupňami ochrany, až sa dostal k svojmu cieľu.

A čo aktualizácie softvérových aplikácií? Sú riešením ochrany pred nežiaducimi prienikmi?

V každom softvéri a hardvéri boli, sú aj budú chyby. Dôležité je, aby boli pravidelne odhaľované a riešené. Jedným z riešení je pravidelné nasadzovanie vydávaných aktualizácií. To sa však ľahko povie, ťažšie urobiť. Každý správca v nejakej väčšej firme, napr. aj v priemyselnom výrobnom podniku, vie, že ak bude bez rozmyslu nasadzovať všetky dostupné aktualizácie a záplaty na všetkých zariadeniach, bude mať síce čisté svedomie, že urobil všetko na zaistenie aktuálnosti a bezpečnosti používaných aplikácií, ale záplaty môžu mať zároveň vplyv na správanie zvyšku daného systému. To znamená, že môj systém nebude mať bezpečnostnú chybu, ale prestane vykonávať tú činnosť, ktorú má. My sa napr. veľmi často stretávame s takou patovou situáciou, keď má radiaci systém nachádzajúci sa v prevádzke nainštalované ovládače k nejakému špecifickému zariadeniu a beží tam operačný systém Windows XP. Ten je už roky nepodporovaný a existuje na ňom celý rad zraniteľností, ktoré sa dajú zneužiť na prienik do daného systému. Všetci to vedia, napriek tomu sa stále používa práve kvôli tomu, že ovládače na špecifický hardvér pre novšie verzie Windows neexistujú. Riešiť takéto situácie nie je ľahké, ale uzavrieť to výrokom „veď aj tak sa s tým nedá nič robiť“ je nesprávne. Dá sa to, ale samotné riešenie nebude možné naformulovať do dvoch viet a nebude určite triviálne.

Ako by teda mali vyzeráť postupy a riešenia v oblasti funkčnej ochrany priemyselných podnikov/prevádzok proti kybernetickým útokom na úrovni HW/SW/ludia? Kto by mal s touto témou v rámci podniku prísť?

V prvom kroku je veľmi dôležité, aby podnik na túto tému delegoval ľudí, pre ktorých bude kybernetická bezpečnosť prioritou. Bez ohľadu na to, kto to bude iniciovať, je dôležitá podpora zo strany najvyššieho vedenia. Kľúčové je, aby nevznikal boj medzi majiteľmi firmy, jej najvyšším vedením a pracovníkmi, ktorí sa majú o kybernetickú bezpečnosť starať. Ak vedenie spoločnosti nebude vnímať hrozbu kybernetického útoku ako problém, tak sa to možno podarí splniť formálne, papierovo, ale nie reálne. Rozdiel medzi tým, ako sa má kybernetická bezpečnosť riešiť, a tým, ako sa to dá predstierať, je veľmi veľký. Úloha budovať kybernetickú bezpečnosť a starať sa o ňu by nemala byť zverená pracovníkom, ktorí majú v podniku aj rôzne ďalšie úlohy a môžu byť v konflikte záujmov. V mnohých prípadoch je bezpečnosť v silnom protiklade

s jednoduchosťou používania. Obmedzenia, ktoré súvisia s riešením kybernetickej bezpečnosti, musia byť využívané len do takej miery, aby bežným pracovníkom neväzovali ruky. Na druhej strane to, že každý má právo prístupu do všetkých sietí a k všetkým systémom, môže znamenať jednoduchosť práce, ale z hľadiska bezpečnosti to nie je v poriadku. No a dôležité je uvedomiť si, že celý proces kybernetickej bezpečnosti sa točí v takom uzavretom kruhu, ktorý zahŕňa prevenciu, detekciu a reakciu. Prevencia ju súbor opatrení na to, aby incident nenastal, resp. aby sme minimalizovali možnosť vzniku incidentu. Do tejto oblasti spadajú organizačné postupy a nastavenia prístupových matíc, SW/HW prostriedky, firewally a pod. Keď sa už napriek týmto opatreniam stane, že útočník nájde slabé miesto a prelomí našu obranu, je dôležité čo najskôr ho odhaliť. Na to slúži detekcia a rôzne systémy bezpečnostného monitoringu. V prípade objavenia sa indikátora útoku informujú o tejto skutočnosti operátora operačného centra bezpečnosti. Súčasťou detekcie môžu byť rôzne pokročilé metódy, napr. honeypot („hriec medu“), čo je vyčlenená časť systému vyzerajúca pre útočníka veľmi lákavo. Ak sa dostane práve na toto miesto, akoby som ho dostal do pasce a mám čas zareagovať na jeho ďalšie aktivity tak, aby som minimalizoval jeho záškodnú činnosť. Po vyhodnotení situácie a zistení, či bola príčina v technike alebo v ľuďoch, u mňa vo firme alebo útok prišiel cez môjho dodávateľa, prichádza tretia fáza – reakcia. V tej treba adekvátne upraviť opatrenia na prevenciu a detekciu.

Je výrobný podnik schopný zvládnuť analýzu, návrh riešenia a celý životný cyklus kybernetickej bezpečnosti sám, alebo je vhodné na riešenie tejto témy prizvať skúsených a nezávislých odborníkov z danej oblasti?

Sám takúto problematiku môže zvládnuť len naozaj veľký podnik, ktorý, ako som už spomínal, by musel mať na to vyčlenených pracovníkov. Téma kybernetickej bezpečnosti je v dnešnej dobe veľmi silná a získať expertov, ktorí vedú pokryť všetky potrebné špecializácie je náročná úloha. Pred dvadsiatimi rokmi vedeli odborníci pokryť veľa tém naraz. Neskôr sa začali špecializovať na konkrétne podoblasti a postupne sú tie špecializácie čoraz užšie. Vybudovanie komplexného riešenia kybernetickej bezpečnosti s internými pracovníkmi nie je pre väčšinu firiem asi veľmi reálna záležitosť. Je oveľa efektívnejšie vybrať si na to skupinu dodávateľov, z ktorých každý je odborník v tej svojej úzkej špecializácii. Dôležité je, aby tam bol jeden koordinátor na integráciu celého riešenia a nezliepalo sa to z izolovaných kúskov.

Čím sa začína proces vytvárania účinného systému na riešenie kybernetickej bezpečnosti?

Na začiatku treba spraviť analýzu GAP, ktorá vytvorí obraz o skutočnom, aktuálnom stave v danej oblasti v podniku a na základe ktorej sa dajú zadefinovať ciele, ku ktorým sa chceme dostať. Ak podnik spadá do už spomínaného zákona o kybernetickej bezpečnosti, minimálne požiadavky sú stanovené práve týmto legislatívnym rámcom. Ak firma pod tento zákon nespadá, možno si zvoliť nejakú osvedčenú normu, resp. riadiť sa najlepšími skúsenosťami z riešenia kybernetickej bezpečnosti v tom sektore, kde podnik pôsobí. Treba si však dať pozor na samotný návrh riešenia, nakoľko možno nasadiť celé spektrum bezpečnostných HW/SW mechanizmov takým spôsobom, že to bude pre daný podnik nezmyselné a budú to vyhodnené prostriedky. Podnik nefunguje preto, aby primárne riešil kybernetickú bezpečnosť, ale preto, čo je základom jeho podnikania. Preto je pri tvorbe koncepcie kybernetickej bezpečnosti vhodné zapojiť do diskusie aj ľudí, ktorí rozumejú biznis modelu a ekonomike danej firmy.

Vyžaduje si projekt kybernetickej bezpečnosti odstávku systémov, alebo ho možno implementovať bez nejakých zásadnejších prerušení činnosti podniku?

Môže sa to líšiť v závislosti od stavu, v akom sa firma nachádza. Ak je firma v stave, že posledných dvadsať rokov nikto problematiku bezpečnosti alebo vôbec inovácií IT infraštruktúry neriešil, tak si to môže vyžiadať aj nejaké prerušenia. Okrem toho treba vnímať aj to, že zavádzaním takýchto riešení budú interní zamestnanci prechádzať určitou zmenou, s ktorou sa budú musieť vyrovnávať. Preto je

dôležité zo strany vedenia správne tieto veci odkomunikovať, aby zamestnanci pochopili význam a zmysel zmeny aj pre nich samých.

Sofistikovanosť a zvyšujúci sa počet kybernetických útokov je znamením, že túto tému by nemal prehliadať nikto – počnúc bežnými občanmi až po veľké korporácie. Aké sú teda trendy a perspektívy v oblasti priemyselnej kybernetickej bezpečnosti aj v súvislosti s nástupom technológií, ako je priemyselný internet vecí, cloud a pod.?

Začnem trochu žartom. To písmenko „s“ v skratke IoT znamená „security“. Len škoda, že to „s“ tam nie je. Čo sa týka priemyselného internetu vecí, tam sa aspoň v nejakej deklaratívnej rovine o bezpečnosti hovorí. Novšie generácie zariadení majú bezpečnostné nástroje vyriešené lepšie, čiže aj tu ten posun vidno. Trend je nasmerovaný dobre, existujú normy, ktoré sa venujú tejto problematike, existujú technologické riešenia, ktoré sú veľmi kvalitné z hľadiska prevencie aj detekcie. Z hľadiska útokov sa trendy dajú rozdeliť, povedzme, na dve kategórie. Prvou sú štátom sponzorované útoky realizované ofenzívnymi vojenskými kybernetickými zložkami, keď sú použité nástroje a techniky vysoko profesionálne. Druhou kategóriou sú komerčné kriminálne aktivity. Uvediem opäť reálny príklad z prostredia EÚ. Firma A vyrábala súčiastky, ktoré dodávala ďalšej firme B a tá ich montovala do svojich finálnych výrobkov. V istom momente vyrobila firma A veľkú sériu súčiastok, ktoré boli dosť kvalitné na to, aby prešli ich internou kontrolou kvality, avšak kontrola kvality u odberateľa zrazu zistila nižšiu kvalitu ako v predchádzajúcom období a nepustila ich na ďalšiu montáž. Po analýze príčin firma A konštatovala, že ich riadiace systémy boli kompromitované cieľovým útokom takým spôsobom, že interne v danej chvíli nebolo možné zistiť zníženú kvalitu. Po objavení sa problémov s dodávateľom pristúpila firma B na odber daného typu súčiastky od iného dodávateľa, nakoľko si nemohla dovoliť prerušiť svoju výrobu. To je konkrétny príklad ekonomickej sabotáže. Ďalším nepríjemným útokom objavujúcim sa už aj v priemyselnom prostredí je nasadenie ransomvéru, ktorý dokáže zablokovať údaje umiestnené na disku, pričom ich spätné získanie je podmienené zaplatením „výkupného“. Objavujú sa infekcie, ktoré obchádzajú domácich používateľov a vyberajú si práve priemyselné podniky.

Je cloud potenciálnou bránou na prienik do priemyselného podniku, ktorý ho využíva?

Cloud je príležitosť aj hrozba. Často prevláda názor, že keď mám údaje v cloude, nemám ich pod kontrolou. Preto firmy často volia riešenie, že ukladajú všetky údaje na svoje interné systémy. No potom je tu otázka, či si dokážem ja sám lepšie zabezpečiť ochranu údajov ako poskytovateľ cloudu. Lebo treba povedať, že tí najznámejší poskytovatelia cloudu, ako Amazon, Microsoft či Google, zamestnávajú tých najlepších odborníkov a čelia denne množstvu rôznych hrozieb, ktoré sú schopní úspešne riešiť. Preto je v mnohých prípadoch oveľa ťažšie úspešne preniknúť do cloudu ako do interného riešenia nejakého podniku. Druhým pohľad je, že ak dôjde k nejakému výpadku na strane poskytovateľa cloudu, podnik s tým nič nedokáže urobiť. Preto sú odôvodnené prípady, keď je pre podnik výhodnejšie mať všetky údaje na svojej infraštruktúre. No to, ktoré riešenie je pre podnik lepšie, je niekedy ťažké identifikovať.

Možno sa dopátrať k útočníkom v prípade priemyselnej sabotáže?

Je to možné, ale je to veľmi náročné. Prípadoch úspešného vypátrania a navyše aj dokázania viny je veľmi málo. Pomer uskutočnených útokov a tých úspešne vypátraných sa počíta rádovo v niekoľkých málo percentách. Niektorí, kto do bezpečnosti neinvestuje, sa oveľa ľahšie stane terčom úspešného útoku, ako ten, kto to systematicky rieši. Zaplácanie možných ciest sťažuje a predražuje celý útok, čo môže nabúrať biznis plán, kvôli ktorému to útočník robí. Ak je totiž zisk z útoku nižší ako prostriedky vynaložené na útok, máme bezpečnosť nastavenú správne. A naopak – pre podnik musí byť bezpečnosť menej nákladná ako potenciálne straty. A to je cieľ.

Ďakujeme za rozhovor.

Anton Gérec

SLEDOVANIE VÝROBY POMOCOU RFID

Spoločnosť Kirschenhofer Maschinen GmbH vyvinula systém riadenia výroby a zabezpečenia kvality pre Britax Römer s použitím RFID nosičov Turck a multiprotokolových modulov TBEN-S-Ethernet v spojení s Labview – bez potreby PLC.

*Nosič veľkosti miniatúr
v základni sedadla bude
v budúcnosti kontrolovať,
ukladať a dokumentovať
výrobný proces.*

To, ako môže byť filozofia Priemyslu 4.0 implementovaná do konkrétnych projektov, predstavila nedávno spoločnosť Kirschenhofer Maschinen GmbH v projekte pre Britax Römer Kindersicherheit GmbH. Kirschenhofer Maschinen implementovala systém sledovania detských sedačiek bez akéhokoľvek druhu nadradených riadiacich systémov alebo centrálnych databáz a pomocou RFID nosiča na produkte ako zásobníka údajov. Tento nosič obsahuje poradie montážnych staníc a dokumentuje všetky výrobné kroky. To zaisťuje kvalitu a umožňuje neskoršiu a ľahšiu identifikáciu produktu aj v jeho obale – na akomkoľvek mieste a bez prístupu k databáze. Úspešný projekt je založený na prepojení TBEN-S viacprotokolových modulov RFID V/V od spoločnosti Turck s Labview, softvérom na vývoj systémov od National Instruments.

Každý, kto niekedy umiestňoval bezpečnostnú autosedačku do auta, ocenil normu Isofix. Stačia dve kliknutia a sedadlo je spoľahlivo upevnené v akomkoľvek vozidle vybavenom upevňovacími bodmi Isofix. Sedadlo má dve permanentne upevnené kotvy, cez ktoré sa dá zacvaknúť do kotviacich bodov vozidla Isofix. Konektor Isofix zjednodušuje konštrukciu sedadla a zvyšuje tak bezpečnosť. Tento „dar z neba“ pre rodičov je výsledkom spolupráce medzi výrobcom detských sedačiek Britax Römer a VW, ktorí spoločne uviedli tento štandard do života. Odvtedy sa stal medzinárodnou požiadavkou pre osobné automobily a detské sedačky.

Zákazníci a výrobcovia venujú osobitnú pozornosť bezpečnosti výrobkov na ochranu detí, ako sú sedadlá na bicykle, prílb, kočíky alebo autosedačky. V tomto prípade nemožno tolerovať žiadne výrobné chyby a musia byť odstránené tak rýchlo, ako je to možné. Avšak to je často mimo dosahu výrobcov, najmä ak dodávatelia dodávajú chybné komponenty. Druhou prioritou je preto zabezpečiť, aby sa stiahnutie výrobkov z obehu vykonalo rýchlo a hladko.

Zjednodušený systém založený na Labview šetrí náklady

Pred zostavením svojej výrobnéj linky pre detskú sedačku Advansafix IV sa spoločnosť Britax Römer poradila s Kirschenhofer Maschinen GmbH, špecialistami na automatizáciu a výrobcami špeciálnych strojov. Obe spoločnosti sa nachádzajú v blízkosti Ulmu, len pár minút jazdy od seba. Spolupráca bola preto aj v doslovnom zmysle slova blízka. Zástupcovia zodpovední na oboch stranách mali čoskoro podobný názor na to, ako by sa mohla automaticky zabezpečiť bezpečnosť prevažne manuálnej výroby novej série detských sedačiek. Riadenie systému malo byť založené na Labview, jednom z najpoužívanejších softvérových prostredí na vývoj systémov pre testovacie, prístrojové a riadiace aplikácie, a nosičoch RFID používaných na ukladanie údajov. Prínosom bolo, že Britax Römer ušetril vysoké náklady na zmenu existujúcej výroby a investície do infraštruktúry.

Výrobný proces Advansafix IV pozostáva zo 16 krokov. V každom z nich sa musí skontrolovať jedna vlastnosť. Začína sa to konštrukciou základne sedadla a končí balením sedadla v kartónovej škatuli. Každý úspešný výrobný krok musí byť zdokumentovaný ako „v poriadku“ (OK). Ak sa nejaká stanica vynechá alebo sa nedá úspešne dokončiť, táto skutočnosť sa označí ako „nie je v poriadku“ (NOK).



Rozhranie TBEN-S-RFID od spoločnosti Turck komunikuje tak cez Profinet s PLC Siemens, ako aj cez Ethernet/IP, čím vytvára rozhranie pre Labview bežiacom na prepracovanej stanici.

Systém sledovania bez PLC a databázy

Nico Dreher, technologický inžinier spoločnosti Britax Römer zodpovedný za projekt, hľadal systém, ktorý by umožnil aj využívanie mobilných zariadení a aplikácií, aby sa zjednodušila identifikácia sedadiel u predajcov. Kirschenhofer vyvinul úplne nový systémový prístup, ktorý by spĺňal obidve požiadavky: riadenie procesu pomocou systému RFID, ktorý uchováva všetky údaje o výrobku na nosiči. Spočiatku sa to nezdá ako niečo prelomové, ale táto forma systému sledovania výroby sa nikdy predtým neimplementovala. Systémy sledovania zvyčajne používajú len ID značky a ukladajú súvisiace výrobné údaje do databázy, ku ktorej možno pristupovať zo všetkých relevantných procesných bodov. Kirschenhofer však chcel ochrániť svojich zákazníkov od tohto typu serverovej infraštruktúry. Koniec koncov, každý predajca by mal mať prístup k databáze. Decentralizovaný systém bez trvalého dátového spojenia a bez PLC má svoje výhody: po prvé mobilitu a nezávislosť a po druhé nižšie náklady. Limitovaná kapacita pamäte nosičov je obmedzenie len na prvý pohľad. Môžu sa ukladať iba relevantné informácie a funkcie.

Ako dôkaz správnej koncepcie sa implementovalo päť centrálnych krokov procesu

Len čo bol pripravený celkový návrh, implementovalo sa do pilotného systému v rámci výrobnéj linky so 16 stanicami ako dôkaz správnosti koncepcie päť kľúčových pozícií. V prvej stanici sa dátový nosič vloží do základnej dosky nasledujúceho sedadla. Čítacia/zapisovacia hlava RFID skontroluje, či je správne uložená, a to tak, že načíta čerstvo nalepený nosič a zapíše ju do obrazu procesu. Ako druhá stanica bola zvolená robotická testovacia bunka. Tá vykonáva vizuálnu kontrolu 16 výrobných funkcií na značne dokončenom sedadle. Ak sa neskôr musia vyrobiť rôzne varianty sedadiel, testovací robot si môže prostredníctvom značky umiestnenej na sedadle zvoliť alternatívny test s inými funkciami. Tretia stanica kontroluje funkciu Isofix. Predtým ako je hotové sedadlo zabalené, štvrtá stanica skontroluje, či všetky predchádzajúce kroky procesu boli na štítku zdokumentované ako OK. Piata stanica je stanica prepracovania, na ktorej sú sedadlá označené ako NOK opravené.

Celý tento proces je uložený na štítku RFID. Existuje len jedno schválené poradie výrobných krokov. Systém zaisťuje, že po úspešnom dokončení procesu montáže na každej zo štyroch staníc sa nastaví správna postupnosť. Stanica 2 teda môže nasledovať len za stanicou 1 (vloženie do štítku). Kontrola, či bol krok na predchádzajúcej stanici 1 úspešne dokončený na aktuálnom sedadle, sa vykonáva na stanici 2. Len potom proces pokračuje.

Lepiace štítky s pamäťou 320 bajtov

Kirschenhofer našiel v spoločnosti Turck tie správne komponenty. Keďže štítok musel byť prilepený priamo na sedadlo, nemohol byť príliš veľký. Takisto to muselo byť relatívne lacné, pretože značka zostáva na výrobku. Spoločnosť Turck mohla ponúknuť inteligentný



Predtým ako je sedadlo vybavené oranžovou nálepkou obsahujúcou sériové číslo, systém skontroluje, či sú všetky procesné stanice na sedadle označené ako OK.

RFID nosič – nálepku TW-L36-18-F-B320, ktorá spĺňa všetky požiadavky. Štítko s veľkosťou 320 bytov dokonca ponúka viac pamäte, než je minimálna požadovaná veľkosť, čo dáva priestor aj na neskoršie vylepšenia systému, ak by sa museli pridať akékoľvek nastavené rozsahy merania alebo viac staníc.

Zjednodušené riešenie bez PLC

Na tento typ systémov sledovania a testovania nie sú potrebné žiadne PLC. Procesy nie sú časovo kritické a môžu byť tiež zaznamenané pomocou konvenčného kancelárskeho hardvéru. Avšak často bývajú v tomto prípade problémom rozhrania. Rozhrania RFID sú normálne určené na pripojenie k priemyselným sieťam ethernet a nemôžu preto ľahko komunikovať s PC aplikáciami alebo mobilnými koncovými zariadeniami.

Craig Craill, spolumajiteľ a programátor PLC v Kirschenhofer, hľadal riešenie, ktoré umožnilo prevádzku systému RFID bez použitia PLC. Najväčšou výzvou bola z tohto pohľadu stanica na prepracovanie. Operátor tu vidí všetky potrebné informácie na tablete. Aplikácia ukazuje, ktorá funkcia je chybná, a zobrazuje referenčný stav montáže v konečnom systéme. Tento systém je založený na štandardnom softvéri, takže spoločnosť Britax dokáže začleniť obrázky a texty bez ďalších nákladov na integráciu. Kirschenhofer využíva na stanici na prepracovanie systém Labview. Nakoľko tento softvér nemal žiadne prepojenie systémom RFID, muselo sa nájsť riešenie.

Naprogramovanie rozhrania medzi Labview a zbernicou Ethernet/IP

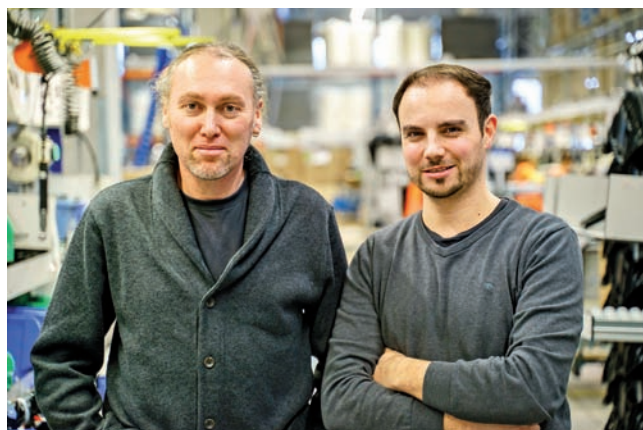
Kirschenhofer vybral kompaktné rozhrania TBEN-S-RFID pre systém Britax Römer a v závislosti od jednotlivých staníc výrobné linky rôzne čítacie/zapisovacie hlavy od spoločnosti Turck. Modul TBEN-S môže poslať údaje z čítacích/zapisovacích hláv RFID predfiltrovateľných cez Profinet, Ethernet/IP alebo Modbus TCP do nadradených systémov, čo sú zvyčajne riadiace systémy. C. Craill sa rozhodol naprogramovať priame rozhranie medzi Labview a Ethernet/IP, aby sa vyhol nepriamej trase cez riadiaci systém. Očakáva pozitívny vývoj protokolu: „Ethernet/IP má veľký potenciál, pretože má výhody priemyselnej siete Ethernet, ale na rozdiel od Profinetu je úplne otvorený a funguje bez licenčných poplatkov. Program tiež kladie vysoký dôraz na potenciál rozhrania medzi Ethernet/IP a Labview, pretože softvér je prakticky priemyselným štandardom pre testovacie zariadenia. C. Craill a jeho kolegovia z Kirschenhofer vytvorili celkovo

900 stránok počas niekoľkých mesiacov, ponorili sa do programov Ethernet/IP a vypracovali súbor s popisom zariadenia pre Labview, ktorý je podobný ovládaču. Predchádzajúce skúsenosti s pilotným systémom potvrdzujú bezproblémovú prevádzku rozhrania a poskytujú Kirschenhoferu slobodu pri ďalších projektoch.

Ďalšou výhodou systému je, že samotný Britax Römer môže definovať ďalšie funkcie, pridať ich do značky a nechať ich skontrolovať. Systém je taký otvorený, že ho možno rozšíriť bez znalosti programovania. Zamestnanci výrobcu sedadiel ho môžu prispôbiť aj rozšíreným výrobným procesom, výrobe iného variantu sedadla alebo dokonca inému výrobku.

Systém založený na značkách šetrí PLC a peniaze

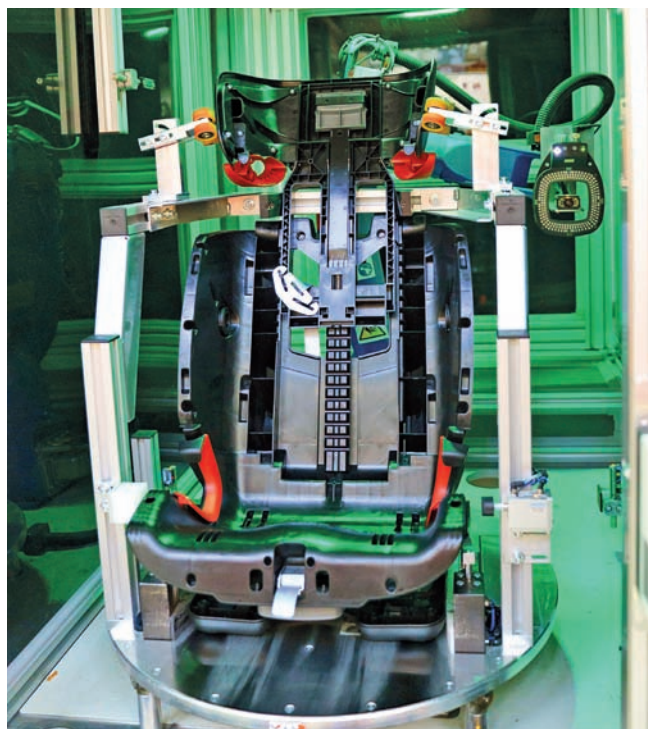
C. Craill zhruba porovnáva cenu riešenia PLC s riešením pre tablet s OS Windows: „Riešenie bez PLC nám umožnilo ušetriť niekoľko tisíc eur na stanici prepracovania. Jednoduchý tablet s OS Windows Surface umožňuje nahradiť PLC, displej a ďalšie IPC na správu databázy.“ Testovací robot je v aktuálnom štádiu nasadzovania stále riadený PLC. Aj tu si C. Craill dokáže predstaviť prácu bez PLC. „To nie je v súčasnosti možné pre bezpečnostné signály. No už som testoval bezpečnostný modul TBPN od spoločnosti Turck. Ten by mohol byť použitý aj na kontrolu testovacieho robota bez potreby PLC.“



Radosť z úspešného projektu: Craig Craill, Kirschenhofer Maschinen GmbH, a Nico Dreher, Britax Römer Kindersicherheit GmbH (vpravo)

Zvýšená bezpečnosť procesu pri prepracovaní

Projekt však nie je vynikajúci len z hľadiska nákladov. Procesy, najmä prepracovanie, sú dnes účinnejšie a bezpečnejšie. „V minulosti bolo potrebné po skúške písomne zaznamenať, aká bola chyba na výrobku, alebo skontrolovať každú funkciu na pracovisku prepracovania. Dnes umiestnime sedadlo do stanice a na displeji uvidíme, ktorá funkcia je chybná. To je značný prínos, pretože je rýchlejší a bezpečnejší ako predtým,“ hovorí N. Dreher, ktorý je nadšený z riešenia. Kirschenhofer vybral pre stanicu prepracovania predĺženú čítaciu/zapisovaciu hlavu TNLQ-Q80L400, pretože pre sedadlo



Čítacia/zapisovacia hlava TTN-Q14, ktorá zapíše výsledok testu na štítko v spodnej časti sedadla, je umiestnená v kovovej podstavci pod ním.



Sedadlo môže byť identifikované v uzavretom obale pomocou vhodnej čítačky RFID – obrovská výhoda aj pri stiahnutí výrobku z trhu.

nie sú k dispozícii žiadne pevné kotviace body a hlava na čítanie/zápis musí pokrývať väčší rozsah. „Dlhšia čítacia/zapisovacia hlava zabezpečuje, že značka je spoľahlivo detegovaná vo všetkých polo-

hách. Stanica tiež umožňuje použitie mobilných zariadení a dokáže rozpoznať sedadlá v uzavretých škatuliach,“ vysvetľuje dôvody výberu čítačky RFID s rozmermi 80 x 400 milimetrov C. Craill.

Použitím riešenia bez PLC sme dokázali ušetriť tisíce eur na stanici prepracovania.

Craig Craill,
Kirschenhofer
Maschinen GmbH

Efektívna logistika výrobkov

Úspešne prepracované sedadlá sa konečne dostanú na poslednú stanicu v rámci výrobnéj linky. Tu sa vykonáva záverečná kontrola, či sú všetky funkcie v poriadku.

Až potom je sedadlo vybavené

schvaľovacím štítkom s jedinečným sériovým číslom. Potom sa zabalí do škatule tak, aby sa štítok mohol prečítať cez kartón bez toho, aby bolo potrebné škatuľu otvoriť. „Môžeme dokonca vytvoriť stanicu prepracovania komunikujúcu s mobilnými zariadeniami. Potrebujeme na to len ďalší tablet, čítačku, prepínač a licenciu Labview. Takto by sme mali absolútny prehľad o prevádzke, boli by sme akcieschopnejší a v prípade poruchy by sme mohli ísť k predajcom a skontrolovať sedadlá. Bolo by to efektívnejšie než to, čo sa robilo predtým,“ hovorí N. Dreher. V takomto prípade sme predtým museli u predajcu vybrať všetky sedačky zo škatúľ, aby sme ich mohli jednoznačne identifikovať. Následne muselo byť každé sedadlo vložené späť a opäť precízne zabalené. To bola náročná úloha pre predajcu aj v našom vlastnom sklade, nakoľko príslušné sedačky museli byť pred odoslaním skontrolované.



Na prvý pohľad: tablet (vpravo) na stanici prepracovania zobrazuje cez Labview, ktorá stanica sa má prepracovať.

Záver

Prevádzka piatich staníc pilotného systému dokazuje platnosť konceptu, ktorý Kirschenhofer implementoval s riešením BL ident RFID od spoločnosti Turck. Projekt má byť teraz spustený na ostatných staniciach. Nie je to prvý projekt, pri ktorom bol C. Craill ohromený komponentmi Turck. „Kirschenhofer už dlho používa moduly TBEN-S. Boli sme prví, ktorí testovali V/V moduly a prví, ktorí používali aj moduly RFID. Boli sme ohromení viacprotokolovým konceptom, pretože nám umožnil držať v sklade len jeden modul. Môžeme to použiť v rámci Profinetu, ako to je v prípade testovacej stanice robota, alebo v Ethernet/IP ako na stanici prepracovania – vždy používame správne zariadenie. Rozsah čítacích a zapisovacích hláv a dátových nosičov nás tiež zaujal. Takýto produktový balík možno nájsť len v spoločnosti Turck.“

Zdroj: Tag Team. Prípadová štúdia. Hans Turck GmbH & Co. KG

Partnerom firmy Turck v SR je Marpex, s.r.o., Dubnica nad Váhom.

-tog-

atp|journal | Aplikácie



MÔJ NÁZOR

BEZ CIEĽA

O ľuďoch bez cieľa sa hovorí ako tých, ktorí nevedia riadiť svoj život. Manažéri podnikov neustále vytyčujú ciele, rozdeľujú ich na jednotlivé oddelenia a ľudí, kontrolujú ich plnenie. Aj ja som si myslel, že ľudský život sa riadi ako projekt, ktorý má cieľ a aktivity na ich dosiahnutie. Už si to nemyslím. Život sa žije a prácu vykonávame najlepšie, ako vieme.

Lao'c napísal: „Ak sa vzdáte cieľov, všetko sa vám podarí. Na svete sú úspešní tí, ktorí sa vzdali cieľov. Pri svojom snažení môžete totiž zabudnúť, že svet je viac ako len víťazstvo.“ Predstavte si, že si nebudeme stanovovať ciele, metriky a postupy na ich dosiahnutie. Jednoducho budeme žiť a robiť veci naplno. Budeme si vyberať to, čo nám dáva zmysel, na čo máme talent, čo nám robí radosť a budeme to robiť najlepšie, ako sa dá. Každú minútu nášho života. Aké ciele dosiahneme? Možno také, aké by sme si ani nedokázali predstaviť. Môžem si dať cieľ, že do pol roka schudnem 10 kilogramov alebo najazdím 3 000 kilometrov na bicykli. A pochybovať si budem plánovať tréningy a zdravú stravu. No môžem na to ísť aj inak – denne si s radosťou zajazdím na bicykli, budem jesť veci, ktoré mi prospeievajú a budem sa tešiť z každého dňa. V prvom prípade možno dosiahnem svoj cieľ, je však otázne, s akým sebazaprením a radosťou. V druhom prípade prežijem pekných šesť mesiacov a je veľká pravdepodobnosť, že schudnem a prejdem niekoľko tisíc kilometrov. Netreba si plánovať veľké veci, stačí robiť s radosťou a naplno drobné veci každý deň.

Nemať ciele neznamená sedieť na mieste a nič nerobiť. Robíme to, čo nám vnútorne robí dobre. Človeku správne veci prospeievajú a nesprávne ho ničia. Ľudia v korporáciách mi oponujú, že bez cieľov sa nedajú dosiahnuť výsledky. Lenže ciele definujú šéfovia, obyčajní pracovníci k nim nemajú žiaden vzťah a ich plnenie je podobné ako veslovanie otrokov na lodi. Som presvedčený, že firmy budúcnosti budú mať menej cieľov a viac radosť z každodennej práce. Bude v nich menej kontrol plnenia cieľov a viac nadšenia z nových nápadov a výsledkov. Menej úsilia sa bude venovať generovaniu ešte vyšších ziskov pre akcionárov a ľudia sa budú viac sústreďovať na to, čo dáva zmysel a čo je prospešné im aj prírode.

Ján Košturiak
IPA Slovakia, s. r. o.

DECENTRALIZOVANÉ RIADENIE S ODOLNÝM PLC

Autonómne elektrické vozíky od firmy Krups Fördersysteme optimalizujú montážnu a testovaciu trať na výrobu batérií nemeckého výrobcu automobilov. Odolné PLC systémy Turck s krytím IP67 zabezpečujú decentralizované riadenie prevádzky jednotlivých modulov dopravníka.

Prostredníctvom systému vozíkov e-Cart reaguje spoločnosť Krups Fördersysteme na zvyšujúce sa požiadavky na modernú automatizáciu procesov montáže a testovania z hľadiska bezpečnosti, nízkej údržby a komunikácie. Trať s potrebou nulovej údržby a inteligentné autonómne vozíky v kombinácii s decentralizovanými systémovými komponentmi so štandardnými ovládacími prvkami zabezpečujú flexibilitu a bezpečnú automatizáciu montáže. To zvyšuje dostupnosť a prináša flexibilitu procesov pre malú veľkosť šarží. Jednotlivé moduly trate sú samostatne riadené TBEN-L-PLC od spoločnosti Turck. S viacprotokolovým PLC s krytím IP67 dokáže Krups ponúknuť štandardné a optimalizované riadiace sekvencie pre jednotlivé komponenty. Zákazníci tak môžu skrátiť čas potrebný na zapojenie a uvedenie do prevádzky a systém ľahko rozšíriť.

Výrobné haly mnohých výrobcov automobilov alebo dodávateľov úrovne 1 sa veľmi podobajú hodinovému mechanizmu. Pracovné úkony robotov a spolupracovníkov na jednotlivých staniciach sú úzko synchronizované, takže spracovaný objekt môže byť potom vrátený do procesného toku. Ak sa však jedno ozubené koleso zadrie, obzvlášť ak je toto ozubené koleso dopravníkom, celá linka vypadne z rytmu.



Systém e-Cart premiestňuje pohon a tým aj údržbu mimo dopravnej dráhy, čím sa maximalizuje jej dostupnosť.

V zozname požiadaviek zákazníkov sú na prvom mieste maximálna dostupnosť a flexibilita. To núti výrobcov dopravníkov zamerať sa na inovácie. Požiadavky smerujú najmä na bezúdržbové a flexibilnejšie dopravníkové systémy, ktoré sa jednoduchšie a rýchlejšie integrujú, ktoré sú lacnejšie a rýchlejšie dostupné ako alternatívne riešenia po kompenzácii všetkých priamych a nepriamych nákladov. Spoločnosť Krups s hlavným závädom v Dernbachu v Porýní-Falcku je jedným z lídrov na trhu v oblasti automatizácie montáže a testovania. Spoločnosť sa špecializuje na automatizačné systémy na efektívne prepojenie montážnych a skúšobných staníc. Nový systém e-Cart predstavuje inteligentné nosiče obrobkov s aktívnym napájaním, ktoré sú schopné otáčať, zdvíhať, upínať alebo nakladať obrobky.

Najnovšie zariadenie Krups je vysoko dostupný dopravníkový systém, ktorý mení zaužívané, resp. vytvára nové príležitosti. Philipp Krups, vedúci spoločnosti už z druhej rodinnej generácie, vysvetľuje základnú myšlienku: „V konvenčnom systéme valčekového dopravníka sa pohon nachádza v dráhe dopravníka. To zahŕňa veľa mechanických častí a ich opotrebenie. Z tohto dôvodu je údržba trvalo inštalovaných systémov vždy problémom. Preto sme chceli vymyslieť úplne nový systém a odstrániť z trate údržbu. Naším výsledkom je pasívna trať, ktorá je úplne bezúdržbová. Celá technológia a elektrický systém sa teraz nachádzajú vo vozíkoch nazývaných e-Carts. Tieto elektricky poháňané vozíky majú samodiagnostickú funkciu a v prípade potreby preventívnej údržby môžu byť mimo prevádzky. To prináša zníženie prestojov a trať zostane prevádzkyschopná. Na dopravníkovom systéme sa v prípade potreby dajú ľahko realizovať akékoľvek neskoršie rozšírenia. Systém e-Cart ďalej umožňuje realizovať flexibilnejšie výrobné procesy s menšou veľkosťou šarží. Dalo by sa dokonca povedať, že ide o dopravník v súlade s koncepciou Priemyslu 4.0.“

e-Cart prináša revolúciu v manipulácii s materiálmi pre elektronickú mobilitu

Krups spustil nový dopravníkový systém pod názvom LOGO! MAT e-Cart. A kde inde, ak nie v automobilovom priemysle by sa mala implementovať jedna z prvých aplikácií tohto systému? Automobilový priemysel je predsa prvým odvetvím, kde sa objavujú nové automatizačné riešenia. Pre Krups je to hračka, pretože spoločnosť má okolo 95 % svojho predaja v automobilovom priemysle. Niektorí zákazníci spoločnosti so sídlom vo Westerwalde sú integrátori, ktorí dodávajú kompletne systémy pre výrobcov automobilov alebo tiež integrátorov samotných výrobcov automobilov. Veľký nemecký výrobca automobilov preto bude v budúcnosti využívať systém e-Cart vo svojom závode na výrobu batérií pre elektromobily.

Aby Krups nemusel znovu vymýšľať koleso, používa modulárny koncept. Systém sa skladá z niekoľkých štandardných modulov: otočné moduly, moduly kyvadlovej dopravy, moduly zastavenia a indexery. Tieto jednotky sú skombinované do návrhu podľa individuálnych požiadaviek zákazníka a prepojené s prevádzkovým riadiacim systémom. Dopravníkový systém poskytuje výrobnému systému zákazníka reportovacie údaje a umožňuje implementáciu obojsmerných komunikačných rozhraní.

Decentralizované riadenie pre modulárne dopravníkové systémy

„Doteraz existoval vždy hlavný riadiaci systém, do ktorého boli smerované všetky signály. To sčasti zahŕňalo zapojenie bod – bod, ale čoraz častejšie aj pripojenie decentralizovaných V/V jednotiek. Problémom bolo programovanie. Programátor zvyčajne programuje všetko v jednej postupnosti. Ak sa však vyskytne nejaká podmienka pri prepnutí alebo po núdzovom spustení, ktorá nie je zastúpená v tejto postupnosti, používatelia musia presunúť jednotky ručne, aby sa obnovila známa situácia,“ vysvetľuje Christian Mies, vývojár riadenia spoločnosti Krups. „Dopravníkový systém musí byť naprogramovaný odlišne, aby sa eliminovala potreba ručných zásahov. Musia byť definované podmienky a vhodné reakcie, ktoré riešia všetky situácie.“ Ak sú moduly riadené v centrálnom riadiacom systéme, musia zákazníci vykonať určité zmeny, ktoré prerušia celkový proces. Ak sa neskôr vyskytnú chyby, posielajú sa do Krups – aj keď za to spoločnosť nebola zodpovedná. Táto skúsenosť naučila Krups jednu vec: v ideálnom prípade by mal byť každý modul riadený samostatne.



„Len privedenie 24 V káblov a signálov do dvanástich riadiacich systémov na záložkách a označenie by bolo veľmi náročné. Cena TBEN-L-PLC to s prehľadom pokrýva,“ konštatuje Christian Mies, Krups Fördersysteme GmbH.

Autonómne riadenie zvyšuje bezpečnosť procesu

V súčasnosti každý modul pracuje externe ako čierna skrinka, ktorá jednoducho komunikuje s centrálnym riadiacim systémom v oboch smeroch cez zbernícové spojenie. Modul spúšťa svoj program, aby vykonával konkrétnu úlohu: otáčanie, prenos, monitorovanie prevádzky a hlásenie stavu modulu. Každý modul je preto riadený – presne podľa vývoja – a dokonale implementuje všetky možné sekvencie. Prevádzkový riadiaci systém je inštalovaný na vyššej úrovni a riadi celkový tok činností. Avšak sekvencie na riadenie skutočnej polohy a monitorovanie podmienok preberá každý riadiaci systém v module.

Krups potom už nemusí zasahovať do riadenia celej prevádzky a naopak, prevádzkový operátor nemusí ovládať moduly dopravníkového systému. Na základnej úrovni musí byť implementovaná len komunikácia medzi hlavným riadiacim systémom a modulmi. Z vnútropodnikového pohľadu komunikuje Krups s týmito modulmi dopravníkových systémov, ktoré majú svoje vlastné inteligentné moduly. Spoločnosť preto pred desiatimi rokmi hľadala autonómne riadiace systémy, ktoré by bolo možné inštalovať priamo na moduly.

Vlastný riadiaci systém s krytím IP67

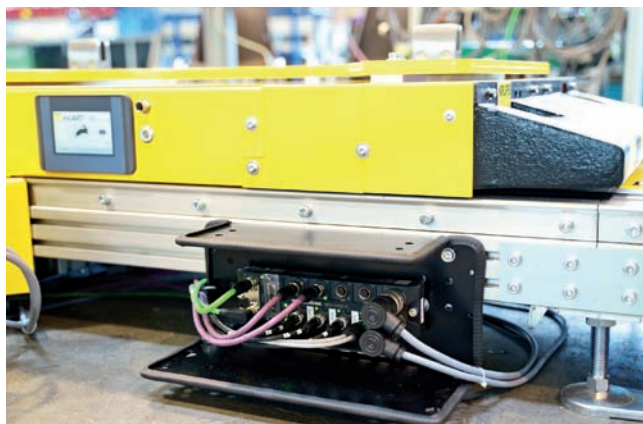
„V tom čase sme už hľadali kompaktné riadiace systémy s krytím IP67. Na trhu však nebolo nič,“ konštatuje Ch. Mies. Krups si v začiatkoch pomohol, ako vedel. „Postavili sme si vlastný riadiaci systém, namontovali sme všetky konektory M12 a umiestnili všetko do puzdra. Toto puzdro muselo mať vŕtacie otvory, pneumatický systém a displej. Išlo o veľmi veľké jednotky a relatívne ťažko sa vyrábali. Museli sme dosky osadiť prvkami, umiestniť do puzdra a všetko



Pred a po: Riadiaci systém zabudovaný v puzdre Krups (vľavo) fungoval dobre, ale v porovnaní s modulom TBEN-L (vpravo) od spoločnosti Turck bol podstatne väčší, náročnejší na inštaláciu a fungoval len v sieťach Profinet.

prepojiť. Hoci to bolo úspešné, bola to náročná úloha, „vysvetlil cestu k vlastnému riadiacemu modulu Peter Krups.

Keďže spoločnosť Turck pred niekoľkými rokmi uviedla na trh blokovaný riadiaci modul TBEN-L-PLC, dokázala si spoločnosť Krups ušetriť námahu potrebnú na vybudovanie vlastného zariadenia. Spoločnosť teraz používa regulátor s krytím IP67 v mnohých modeloch strojov – nielen v systéme e-Cart. Riadiaci systém pre každý prvok dopravníkového systému bol naprogramovaný v Codesys. Komunikácia s pohonmi alebo blokmi ventilov a ďalšími komponentmi modulu sa realizuje cez zbernícové rozhranie, pričom komunikácia s hlavným regulátorom je väčšinou realizovaná cez Profinet. „Teraz máme tú výhodu, že moduly môžu byť nasadené okamžite a bez potreby akéhokoľvek iného programovacieho prevádzkového zariadenia, t. j. nahradiť, vložiť, zálohovať dáta. V ideálnom prípade musí zákazník pripojiť len 7/8-palcový konektor pre 24 voltov a ethernetový konektor na pripojenie zbernice,“ vysvetľuje Ch. Mies výhody pre používateľov. Pre medzinárodnú spoločnosť, ako je Krups, sa podľa manažéra IT Ch. Miesy vyplatí aj rad protokolov, ktoré kompaktný riadiaci systém ponúka. „Americkému trhu dokážeme ponúknuť verziu s Ethernet/IP, rovnako aj pre európsky a ázijský trh, kde sú protokoly zmiešané. V súčasnosti sa sústreďujeme na Ethernet/IP a Profinet, ale ak to vyžaduje zákazník, vieme ponúknuť aj Modbus TCP. Veľkou výhodou je aj skutočnosť, že všetky licencie Codesys sú obsiahnuté v zariadení Turck. Licencia je tam a môžeme ju používať bez ohľadu na to, ktorú zbernicu zákazník používa. Môžeme ich dokonca použiť vtedy, keď potrebujeme malý hlavný riadiaci systém, pretože k dispozícii sú aj master licencie,“ opisuje Ch. Mies rôzne scenáre, v ktorých môže byť TBEN-L-PLC nasadený.



TBEN-L-PLC od Turck ovláda moduly dopravníkov Krups – komunikáciu s perifériou zabezpečuje zbernica CAN a s hlavným riadiacim systémom zbernice Profinet alebo Ethernet/IP.

Systém e-Cart šetrí energiu pri výrobe batérií

Technické vlastnosti dopravníkového systému e-Cart pri výrobe batérií už dávajú jasne najavo, že výrobca s e-mobilitou počíta. So 130



Na zarážkach a ďalších funkčných moduloch komunikuje systém e-Cart s vozíkmi cez NFC.

samohybnými vozíkmi na dĺžke jeden kilometer dopravnej dráhy sa nízkosériová výroba nerozbehla. Krups na trati osadil 70 točníc a okolo 140 zarážok. Desať zarážok používa TBEN-L-PLC spoločne ako bránu k hlavnému riadiacemu systému zákazníka. To značne znižuje počet uzlov zbernice, ktoré sú potrebné pre zákazníka.

Na zmenu smeru sa vozíky premiestňujú na paralelné trasy alebo sa ich smer mení točnicami. Na rozdiel od väčšiny konvenčných systémov možno s vozíkmi systému e-Cart priamo komunikovať. Aby bolo možné použiť TBEN-L-PLC ako bránu na implementáciu komunikácie medzi hlavným riadiacim systémom a vozíkmi, sú zarážky vybavené jednotkami s komunikáciou NFC (Near Field Communication). Týmto spôsobom môžu byť vozíky odstránené v závislosti od ich stavu alebo výskytu výstražných správ. Ďalšou výhodou je, že vozíky v stave čakania nespotrebovávajú žiadnu energiu – na rozdiel od konvenčných systémov valčekových dopravníkov, v ktorých pohony normálne pokračujú v chode –, aj keď sa nepohybujú žiadne kartóny.

BL compact poskytuje dodatočné V/V cez CAN

K TBEN-L-PLC sú priamo pripojené aj snímače a ovládače modulov. Blokový riadiaci systém poskytuje osem univerzálnych kanálov na štyroch zásuvkách, ktoré možno automaticky nastaviť na požadovanú konfiguráciu ako vstup alebo výstup. Ak sú potrebné iné V/V, Krups dokáže rozšíriť počet potrebných signálov so V/V modulom BL compact prostredníctvom zbernice CAN. Moduly BL compact sú tiež navrhnuté s krytím IP67 a montujú sa priamo na jednotky.

IP67 šetrí kabeláž

Krups zistil, že vďaka technológii IP67 možno ušetriť množstvo práce. „Len privedenie 24 V káblov a signálov do dvanástich riadiacich systémov na zarážkach a ich označenie by bolo veľmi náročné. Cena TBEN-L-PLC to s prehľadom pokrýva,“ oceňuje Ch. Mies.

Systém e-Cart je nielen energeticky úsporný a odolný proti poruchám, ale umožňuje aj flexibilnejšie procesy, ako je uvedené v modelových scenároch Priemyslu 4.0 a aj tých, ktoré už boli implementované. Prostredníctvom komunikácie s nosičmi obrobkov možno dosiahnuť väčšiu rôznorodosť produktov, ako uvádza ďalší príklad použitia. Podobne ako v automobilovom priemysle,



„Z dlhodobého hľadiska nechceme byť len dodávateľom mechanických systémov, ale aj dopravníkových systémov typu „pripoj a funguj“ – inteligentných systémov, ktoré sa samy riadia a potrebujú len nadradený riadiaci systém,“ hovorí Philipp Krups.

dopravuje systém e-Cart nápravy vozidiel dvoch modelov. Existuje však 140 rôznych typov náprav, ktoré môžu vozíky v rámci výroby prepravovať. Aktívne poháňané nosiče obrobkov umožňujú jednoduché vykonanie alebo vynechanie rôznych výrobných krokov. Tým sa minimalizuje čakací čas a vozíkom na jednotlivých staniciach môže byť priradená rôzna rýchlosť.

Systém e-Cart s inteligentnou riadiacou technológiou tak pomáha zabezpečiť hladký a vysoko efektívny výkon flexibilných výrobných procesov. Vzhľadom na to všetko je jasné, že obraz výroby ako dobre synchronizovaného hodinového stroja pochádza z iného času. Aj keď produkcia 4.0 vyžaduje presné zapadnutie jedného ozubeného kolesa do druhého, hodiny výroby 4.0 musia byť flexibilné ako hodiny v obrazoch Salvadora Dalího.

Zdroj: Cart Track 4.0. Prípadová štúdia. Hans Turck GmbH & Co. KG.

Partnerom firmy Turck v SR je Marpex, s.r.o., Dubnica nad Váhom.

-tog-

Spoločnosť GRISARD BITUMEN AG je na švajčiarskom trhu bitúmenov známa už 100 rokov. Vyvíja, rafinuje a distribuuje bitúmenové lepidlá vysokej kvality. Vo svojich vlastných laboratóriách vyvíja bitúmeny podľa želania zákazníka, ktoré sa používajú na výstavbu ciest, letísk a dráh, ako aj pri výrobe dechtového papiera a v emulznom priemysle.

NAJVYŠŠIA PRESNOSŤ PRI PLNENÍ VISKÓZNEHO BITÚMENU

Meranie vysoko viskózneho bitúmenu vyžaduje najvyššie štandardy meracej techniky. Počas predchádzajúcich rokov sme zistili, že Endress+Hauser je pre túto oblasť kvalifikovaným a spoľahlivým partnerom. Obzvlášť rozhodujúca bola veľmi úzka a dobrá spolupráca so servisným technikom. Vďaka tomu sme boli schopní nájsť perfektné riešenie na presné plnenie cisternových vozidiel s inovatívnym Coriolisovým prietokomerom Promass Q 500.

Eduard Martini
generálny riaditeľ BITUTANK AG, Švajčiarsko

Na naplnenie cisterien s vysoko kvalitným bitúmenom používa GRISARD BITUMEN AG váhu na meranie hmotnosti nákladných vozidiel a nový Coriolisov prietokomer Promass Q 500. To umožňuje merať asfalt, ktorý niekedy obsahuje plyny, s bezprecedentnou presnosťou.

Výsledky:

- zníženie chyby merania z maximálne 8 % na 0,1 až 0,2 %,
- väčšia dostupnosť prevádzky vďaka spracovaniu údajov dostupných cez internet

Výzva zákazníka

Bežné bitúmeny dodávané loďou BITUTANK AG sa prepravujú do rôznych skladovacích nádrží cez vyhrievané rúry (170 °C), rafinované prísadami na výrobu bitúmenu modifikovaného polymérom (PmB), a potom k zákazníkovi po železnici alebo cisternovými autami. V minulosti sa množstvo bitúmenu naplneného do cisternových vozidiel určovalo pomocou váhy na váženie nákladných vozidiel a iného typu Coriolisovho prietokomera.

V dôsledku procesu odplyňovania vo vysoko viskóznom bitúmene však tento starší prietokomer vykazoval chyby merania až 8 % v porovnaní s váhou na meranie hmotnosti nákladného vozidla (napr. až 2 tony pri celkovom plnení 25 ton). Pretože miesto merania prietoku sa v závislosti od systému nachádza na strane výtlaku aj

na strane nasávania čerpadla, v dôsledku kolísania tlaku sú procesy odplyňovania normálne.

Preto bolo potrebné hľadať takú technológiu merania prietoku, ktorá zabezpečí najvyššiu presnosť plnenia viskózných kvapalín a nie je citlivá na výkyvy prevádzkového tlaku a prítomnosť plynu. Ďalšou požiadavkou založenou na potrebe lepšej dostupnosti prevádzky bolo umožniť ukladanie, vyhodnocovanie a získavanie všetkých nameraných údajov pomocou cloudového riešenia využívajúceho internet.

Riešenie

Namiesto pôvodného Coriolisovho prietokomera bol na bitúmenovej čerpacej stanici nainštalovaný Promass Q 500, novo vyvinutý firmou Endress+Hauser. Jeho prednosťami boli najmä:

- vynikajúce výkonové charakteristiky pre obchodné prípady zahŕňajúce prenos látok od jedného operátora k druhému a/alebo fakturačné merania,
- meranie je prakticky nezávislé od kolísania procesných tlakov a teplôt,
- súčasné meranie hmotnosti, objemu, hustoty a teploty,
- patentovaná „viacfrekvenčná technológia“ (MFT) na spoľahlivé meranie kvapalín obsahujúcich strhávané plyny alebo mikrobublinky.



Prietokomer Promass
s technológiou Heartbeat



Zariadenia na nakladanie
skvapalneného bitúmenu

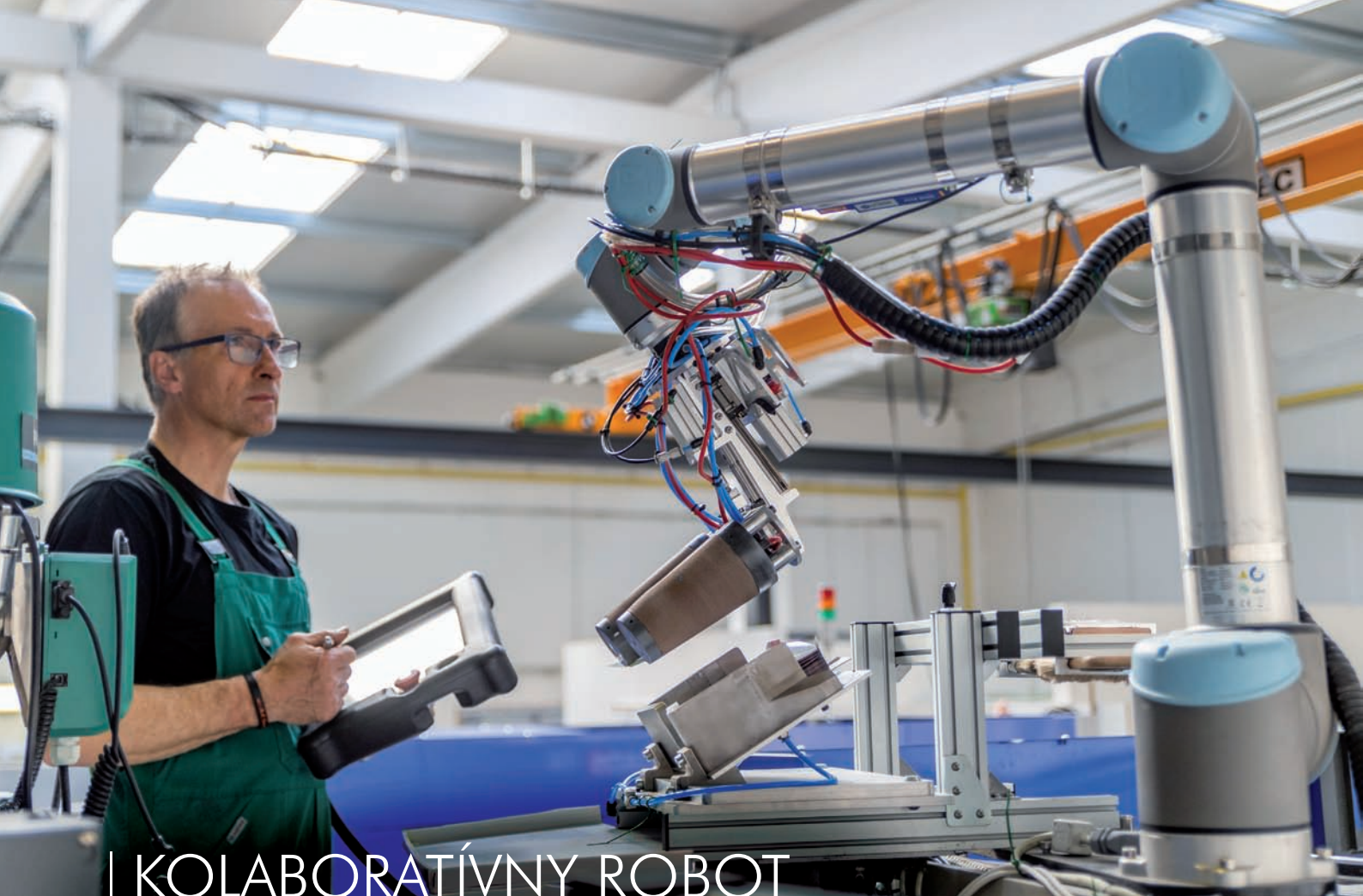


Čerpacia stanica bitúmenu s prietokomerom Promass
nasadeným v prevádzke

Na prediktívnu analýzu a údržbu údajov získavaných a vyhodnocovaných v cloudovom prostredí a dostupných cez internet vyvinula Spoločnosť Endress+Hauser softvérové riešenie IIoT špeciálne prispôbené potrebám zákazníkov. Umožňuje:

- celosvetový prístup k všetkým nameraným údajom aktuálnych alebo predchádzajúcich ukončených procesov plnenia,
- rôzne možnosti hodnotenia, napr. trendové analýzy parametrov procesu a/alebo kvality, ako je hmotnosť, objem, hustota, koncentrácia, teplota atď.,
- využiť technológiu Heartbeat na detekciu zmien v procese a/alebo zariadení, napr. prostredníctvom kavitácie, nahromadenia, oderu/korózie či nehomogénnych kvapalín.

www.transcom.sk



KOLABORATÍVNY ROBOT POMOHOL URÝCHLIŤ A ZEFEKTÍVNIŤ VÝROBU

Spoločnosť 2D & S, s. r. o., sa zaoberá lisovaním termoplastických látok a výrobou nástrojov na lisovanie týchto materiálov. 2D & S so sídlom v Kuřimi ponúka svojim zákazníkom komplexné služby, ktoré zahŕňajú okrem iného aj spracovanie návrhu modelu produktu pomocou konštrukčného softvéru. Firma venuje, okrem iného, veľkú pozornosť skracovaniu dodacích termínov pri udržaní vysokej kvality finálnych výrobkov.

Výzvy

„V poslednom čase sa najväčšou výzvou pre našu spoločnosť stala efektívnosť práce, zvýšenie produktivity a dosiahnutie čo najkratších výrobných cyklov,“ hovorí David Dědek, konateľ spoločnosti 2D & S, s. r. o. Rastúce požiadavky zo strany zákazníkov na rýchlosť a kvalitu výrobkov viedli spoločnosť k rozhodnutiu úplne zautomatizovať lisovací stroj na termoplastické látky. Dôležité bolo tiež eliminovať náklady na prípadné stavebné úpravy výrobného haly, čo by vyžadovalo obstaranie štandardného priemyselného robota.

Riešenie

Na základe mnohých pozitívnych referencií sa spoločnosť rozhodla zakúpiť kolaboratívny robot UR10 od Universal Robots, ktorý spĺňa najnáročnejšie predpoklady spoľahlivej integrácie do existujúceho výrobného procesu. Primárne je robot UR10 určený na zakladanie IML (in-mould labelling) fólií do formy na plastový výlisok. Pri technológii IML je viacvrstváová fólia počas výroby zaliata plastom. Pri aplikácii plastu je etiketa zo zadnej strany zalievaná roztaveným

plastom a tým fixovaná na vonkajšiu stranu formy. Čiastočným natanením príľne IML fólia spoľahlivo k plastu. Fólia sa tak stane neoddeliteľnou súčasťou finálneho produktu, napríklad vratného plastového téglika, s ktorým sa môžeme stretnúť na akciách alebo festivaloch pod otvoreným nebom.

Výroba takýchto téglikov je veľmi monotónna činnosť, ktorá však vyžaduje veľkú presnosť pri manipulácii a zakladaní plastových fólií do formy. Pracovisko, kde je robot umiestnený, musí umožňovať spoluprácu človeka s robotom, pretože ľudský pracovník zakladá fólie do pripraveného zásobníka, z ktorého robot následne berie IML fólie. Vzhľadom na veľkosť tiež treba prekonať pomerne veľkú vzdialenosť zo zásobníka fólií priamo do vnútra vstrekovacieho stroja. Na to je ideálnou voľbou kolaboratívny robot Universal Robots s veľkým pracovným rozsahom ramena.

„Výroba plastových téglikov sa dramaticky zrýchlila. Na začiatku sme mali drobné problémy s nastavením presnosti, ktoré boli veľmi rýchlo vyriešené. Teraz môžeme hrdlo povedať, že si už nedokážeme bez kolaboratívneho robota výrobu predstaviť,“ hovorí Jiří Kašparec, operátor výroby v spoločnosti 2D & S, s. r. o.

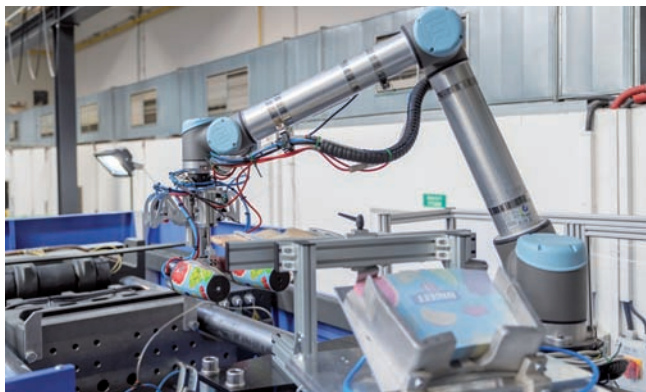


Prínosy

Kolaboratívny robot UR10 podstatne zrýchlil výrobu plastových výliskov. Momentálne spoločnosť používa šesťosový kolaboratívny robot od Universal Robots na jednom vstrekovacom stroji. Zároveň sa usilovne pracuje na rozšírení výroby a rozvoji firmy, ktoré si vyžaduje plánované obstaranie ďalších dvoch kolaboratívnych robotov.

Spokojnosť zákazníka

„Doteraz sme nemali žiadne robotizované pracoviská, a preto sme mali pred zaobstaraním mierne obavy najmä ohľadom spoľahlivosti a nasadenia kolaboratívnych robotov. Prebehlo plánované profesionálne preškolenie našich zamestnancov spoločnosťou Universal Robots, ktoré bolo veľkým prínosom pre rozbeh výroby s týmto pre nás novým zariadením. Vďaka perfektne predpripravenému programu od firmy MP LINE sa výroba veľmi rýchlo rozbehla, pričom zo strany našich operátorov prebehli len drobné editácie a úpravy programu. Integrácia kolaboratívneho robota do procesu výroby nás príjemne prekvapila najmä vďaka rýchlosti a jednoduchosti,“ konštatuje D. Dědek, konateľ spoločnosti 2D & S, s. r. o.



Spoločný systémový integrátor

Dlhoročné skúsenosti v oblasti automatizácie výroby, najmä periférií k vstrekovacím strojom, nasmerovali spoločnosť MP LINE, s. r. o., na poskytovanie komplexných a spoľahlivých riešení s cieľom zefektívnenia výrobných procesov firiem. Využitím moderných technológií a metód dokáže spoločnosť navrhovať a integrovať proces automatizácie do rôznych priemyselných odborov a zabezpečiť tak efektívny proces výroby. Jednou z oblastí jej činnosti je integrácia riešení Universal Robots, kde sa stala rešpektovaným integrátorom a prvým certifikovaným integrátorom UR v Českej republike.



UNIVERSAL ROBOTS

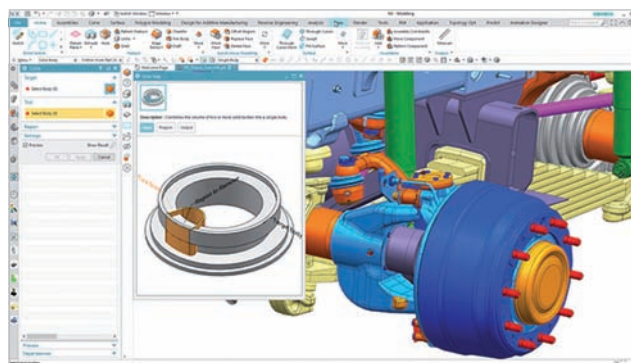
Universal Robots A/S

Siemensova 2717/4
155 00 Praha 13 – Stodůlky
www.universal-robots.cz

|atp|journal | Aplikácie

UMELÁ INTELIGENCIA A STROJOVÉ UČENIE AKO PODPORA NÁVRHU PRODUKTOV A RIEŠENÍ

Spoločnosť Siemens vo februári tohto roku oznámila rozšírenie platformy Digital Innovation Platform o najnovšiu verziu softvéru NX™, ktorá bola doplnená o schopnosti strojového učenia a umelej inteligencie. Tieto nové funkcie dokážu predpovedať ďalšie kroky a aktualizovať používateľské rozhranie s cieľom pomôcť používateľom efektívnejšie využívať softvér na zvýšenie produktivity. Schopnosť automaticky prispôbiť používateľské rozhranie potrebám rôznych typov používateľov vo viacerých oddeleniach môže viesť k vyššej miere prijatia, čo povedie k vyššej kvalite CAx systémov a vytvoreniu presnejších digitálnych dvojčiat.



Strojové učenie sa čoraz viac využíva v procese návrhu produktov, aby poskytlo konkurenčnú výhodu. Túto technológiu možno využiť na rýchlejšie a efektívnejšie poskytovanie cenných obchodných informácií, pričom dokáže spracovávať, analyzovať a učiť sa z veľkých objemov dát. Umeľá inteligencia a strojové učenie možno použiť aj na monitorovanie správania sa používateľa a jeho úspechov a zlyhaní, alebo na modifikáciu rozhrania a využitie poznatkov o používaní UI pre personalizáciu prostredia CAx.

„V rámci CAD nástrojov vždy existoval kompromis medzi funkčnosťou a použiteľnosťou. Čím viac sa tieto nástroje rozširujú, tým náročnejšie sú na používanie a ovládanie,“ povedal Chad Jackson, hlavný analytik spoločnosti Lifecycle Insights. „Adaptívna umelá inteligencia je odpoveďou na túto otázku. Navádza nových aj starých používateľov k využívaniu správnej funkčnosti v správnom čase. A väčšina z nich má z toho prospech.“

Digital Innovation Platform spoločnosti Siemens sa neustále rozširuje a umožňuje zákazníkom vytvárať najpresnejšie digitálne dvojčatá produktov, výrobných prevádzok a výkonu produktu. Integrácia strojového učenia a umelej inteligencie do softvéru NX ponúka výhody plynúce z rýchlosti, výkonu, efektivity a inteligencie prostredníctvom učenia, bez toho, aby ste museli tieto vlastnosti explicitne naprogramovať. To ponúka zákazníkom veľa príležitostí na zlepšenie procesu navrhovania a v konečnom dôsledku ich ponuky a skrátenia času uvedenia na trh. Modul NX Command Prediction je prvou lastovičkou adaptívneho používateľského rozhrania s podporou strojového učenia na trhu a bude základom pre ďalšie používateľské riešenia založené na strojovom učení.

„Hoci rozsiahly výskum v oblasti interakcie človek-počítač vyústil do vynikajúceho statického rozhrania, stále nám chýba dokonale prispôsobiteľné dynamické rozhranie, ktoré môže vyhovovať všetkým používateľom,“ povedal Bob Haubrock, senior viceprezident spoločnosti Product Engineering Software spoločnosti Siemens PLM softvér. „Najnovšia verzia NX využíva strojové učenie a umelú inteligenciu na monitorovanie činností používateľa a ich úspechov a chýb, takže teraz môžeme dynamicky určovať, ako využívať správne príkazy v rámci NX alebo upraviť rozhranie tak, aby bol každý používateľ produktívnejší. Využitie týchto poznatkov o používateľskom rozhraní pre personalizáciu prostredia CAx môže pomôcť našim zákazníkom zlepšiť celkové využitie a mieru prijatia, čo nakoniec povedie k efektívnejším procesom vývoja produktov.“

www.siemens.com

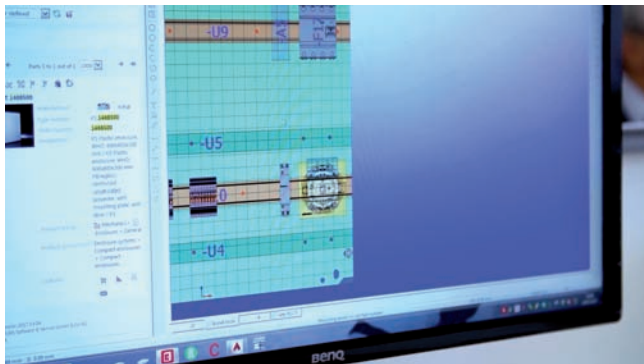
EPLAN PRO PANEL A RITTAL PERFOREX – VÍTAZNÁ KOMBINÁCIA!

Keď spoločnosť Burnell Switchgear and Control, špecialista na distribúciu energie, potrebovala pomoc s narastajúcou produktivitou, aby sa vyrovnala s rýchlo rastúcim dopytom po svojich produktoch a službách, obrátila sa na spoločnosť EPLAN. Technici spoločnosti EPLAN čoskoro zistili, že nielen program EPLAN Pro Panel CAE prináša veľké úspory času v oblasti inžinierstva a návrhu, ale úplne automatizované obrábacie centrum Rittal Perforex by prinieslo rovnako významné časové úspory pre výrobné operácie.

Burnell Switchgear and Control ponúka mimoriadne dôležité riešenia pre distribúciu energie založené na kompletne certifikovaných a akreditovaných systémoch. Silný a trvalý rast dopytu po ich výrobkoch znamenal, že spoločnosť potrebovala znížiť čas potrebný na konštrukciu a výrobu, aby sa zvýšila kapacita. Vedenie spoločnosti Burnell Switchgear and Controls rozhodlo, že riešením by mohla byť implementácia systému CAE, a požiadalo EPLAN, aby im poradil. „Bolo to jednoduché rozhodnutie spojiť sa s EPLAN, pretože spoločnosť je lídrom v oblasti CAE. Po tom, čo sa inžinieri spoločnosti EPLAN pozreli na naše požiadavky, navrhli, že by sme mali navštíviť inovačné centrum Rittal v Nemecku, aby sme mohli vidieť výhody EPLAN Pro Panel a tiež obrábacieho centra Rittal Perforex.“

EPLAN Pro Panel umožňuje technikom navrhnuť a vytvoriť rozvádzače a ovládacie panely. Spracúva kompletne káblovanie, montáž komponentov a detaily konfigurácie zberníc a vytvára 3D pohľady, takže technici a zákazníci môžu presne vidieť, ako budú hotové panely vyzerieť, ešte pred začatím prác na ich stavbe.

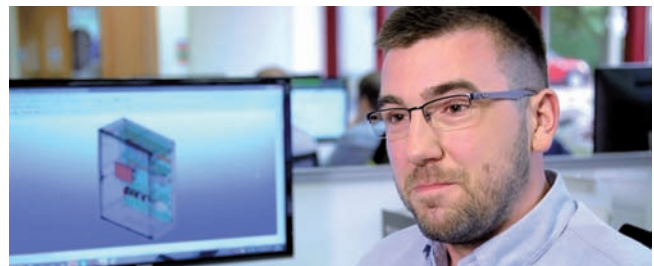
Virtuálny 3D model rozvádzača pomáha vývojárom čo najlepšie využiť cenný priestor ovládacieho panela. Integrované pomôcky pri plánovaní, ako sú kolízne skúšky, dodržiavanie montážnych pokynov výrobcu, minimálna vzdialenosť a polomer ohybu, umožňujú rýchle a optimálne umiestnenie a inštaláciu.



Virtuálny 3D model rozvádzača pomáha vývojárom čo najlepšie využiť cenný priestor ovládacieho panela.

EPLAN Pro Panel navrhnutý s ohľadom na maximálnu flexibilitu umožňuje používateľovi vybrať si preferovaný prístup, či už je založený na zoznamoch zariadení, zoznamoch pripojení, alebo schémach obvodov. Vďaka inovatívnej technológii eTouch možno všetky potrebné komponenty jednoducho zadať a umiestniť v rámci 3D návrhu. „Počas našej návštevy v inovačnom centre Rittal v Nemecku sme si vyskúšali obrábacie centrum Rittal Perforex, ktoré automaticky vyvrtá diery a odrezáva otvory v krytoch, dverách a montážnych doskách pomocou údajov vytvorených v EPLAN Pro Panel,“ povedal P. Wozniak. „Keď sme videli stroj v akcii, nebolo ťažké rozhodnúť sa, že ho potrebujeme. Nakoniec sme nakúpili licencie pre EPLAN Pro Panel a stroj Rittal Perforex!“

Perforex je CNC stroj šitý na mieru výzvam výroby rozvádzačov. Je ideálny na automatizovanú výrobu otvorov a výrezov v plechu a dokáže tiež poklepať otvory na uľahčenie montáže komponentov. Stroje Rittal Perforex sú vhodné pre všetky materiály, ktoré sa zvyčajne nachádzajú v rozvádzačoch a radiaciach paneloch, vrátane ocele, hliníka, medi a plastov. Okrem toho automaticky mení



„S EPLAN Pro Panel a strojom Perforex sme výrazne zvýšili našu produktivitu a kapacitu,“ hovorí s nadšením P. Wozniak.

nástrojov umožňuje vykonávať viacero úloh v jednej operácii bez potreby zásahu operátora. Import údajov návrhu priamo z vývojárskeho softvéru EPLAN Pro Panel ešte viac zvyšuje produktivitu. „V porovnaní s tradičnými ručnými metódami pri výrobe rozvádzačov a ovládacích panelov poskytuje Rittal Perforex výrazne vyššiu efektívnosť a produktivitu. Spoločnosť nás informovala, že príprava dverí, ktorá zaberala aspoň 8 hodín práce s ručným náradím, trvá na stroji Perforex vlastne len 15 minút,“ povedal Jarett Lathey, regionálny manažér predaja spoločnosti EPLAN.

Okrem EPLAN Pro Panel a Rittal Perforex používajú v Burnell Switchgear a Controls aj EPLAN Data Portal, webovú platformu s informáciami od významných dodávateľov elektrických, mechanických, fluidných a pneumatických produktov. Technikom spoločnosti Burnell to poskytuje okamžitý prístup k presným a aktuálnym informáciám takmer o všetkých komponentoch, ktoré používajú vo svojich systémoch, vo formáte, ktorý je priamo použiteľný v programe EPLAN Pro Panel. EPLAN Data Portal sa neustále rozširuje, v čase prípravy tohto článku obsahoval údaje o viac ako 800 000 komponentov od viac ako 220 výrobcov.

Spoločnosť Burnell Switchgear a Controls má v súčasnosti troch vyškolených technikov, ktorí používajú EPLAN na plný úväzok. Spoločnosť očakáva, že do konca roka bude mať šesť plne vyškolených špecialistov EPLAN a už zakúpila ďalších 20 dní školenia. „S EPLAN Pro Panel a strojom Perforex sme výrazne zvýšili našu produktivitu a kapacitu,“ hovorí s nadšením P. Wozniak. Vďaka tejto víťaznej kombinácii – EPLAN Pro Panel, Rittal Perforex a EPLAN Data Portal – teraz zvyšujeme náskok pred našimi konkurentmi a prechádzame na vyšší výkon.“



Pozrite si aj sprievodné video k tejto prípadovej štúdií.



EPLAN Software & Services

www.eplan-sk.sk

OBO CONSTRUCT

OBO Construct predstavuje softvérové riešenia a projekčné aplikácie pre rôzne oblasti elektroinštalácií:

- káblové nosné systémy (nadstavba pre AutoCAD, pomôcka pri výbere správneho nosného systému),
- systémy prepäťovej ochrany (výberová pomôcka k systémom ochrany pred prepätím),
- systémy protipožiarnej ochrany (projekčná, resp. výberová pomôcka pre systémy protipožiarneho prestupu a upchávok),
- podlahové systémy (projekčná, resp. výberová pomôcka pre podlahové systémy).

Výpočet množství

Stavební díl	Masivní stěna
Uložení kabelů	Kabelové nosné systémy
Požární odolnost	90 min.
Druh otvoru	Rohový
Počet přepážek	1
Šířka x výška [cm]	20 x 30
Kabelová zátěž [%]	25
Potřebná přepážková hmota [kg]	6.75
Počet pytlů à 20 kg	0.34
Přidat do nákupního seznamu	

Prvky systému



Protipožární malta pro kombinovanou přepážku MSX-E1



Protipožární malta pro kombinovanou přepážku MSX-S1



NDK-S

Příklad návrhu materiálu v aplikaci OBO Construct BSS

S OBO Construct můžete projektovat v souladu s konkrétními požiadavkami projektu. Aplikácie vás na mnohých miestach krok za krokom privedú až k vhodnému výrobku. Jednotlivé moduly sa riadia technickými predpismi a normami, čo je dôležité najmä pri projektovaní systému protipožiarnej a prepäťovej ochrany. Aplikácie sú dostupné zdarma pre rôzne platformy:

- aplikácie pre mobilné zariadenia,
- aplikácie online v prehliadači,
- samostatné aplikácie pre Windows.



OBO Construct pre jednotlivé systémy OBO Bettermann môžete bezplatne používať online, prípadne si ho môžete stiahnuť z našej webovej stránky <https://obo.cz/cs-cz/podpora/OBO-Construct-4858.html>.

Aplikácie na projektovanie protipožiarneho systému (BSS)

Protipožiarne ochrany stavia dnes mnohých realizátorov technického vybavenia budov pred zdanlivo neprekonateľnými prekážkami. Tento online nástroj vám pomôže vybrať vhodné protipožiarne systémy pre vaše projekty.

Výhody:

- výber správneho výrobku na konkrétne riešenie prestupu,
- rýchla a jednoduchá navigácia,
- nezávislosť od konkrétnej platformy,
- presný zoznam výmer vo formáte Excel.

www.obo.sk



Prepojovacie kanály VK

- ✓ osvedčená kvalita s výrezmi bez otrepov
- ✓ zaoblené jazýčky zabraňujú poraneniu
- ✓ stabilné kanály s veľkou hrúbkou stien
- ✓ presné miesta požadovaného zlomu prepážok a dna
- ✓ skúšané podľa VDE, UL file no. E301798
- ✓ bezhalogénové kanály z kvalitného PC/ABS

Building Connections

www.obo.sk

SYSTÉM RIADENIA PRIEMYSELNEJ KYBERNETICKEJ BEZPEČNOSTI

Implementácia priemyselnej kybernetickej bezpečnosti v podniku nie je len o jednorazovom aplikovaní technických opatrení na zníženie rizika pred kybernetickým incidentom v súlade s medzinárodne uznávanými normami. Je to hlavne trvalý proces, ktorý si zasluhuje pozornosť počas celého svojho životného cyklu. Skúsenosti z praxe v slovenských priemyselných podnikoch ukázali, že úspešné nasadenie riešenia kybernetickej bezpečnosti je o úzkej spolupráci viacerých odborníkov na strane dodávateľa riešenia aj na strane samotného priemyselného podniku.

Prevádzkové technológie (Operational Technology – OT) sa dlho považovali za bezpečný priestor, ktorého sa kybernetická bezpečnosť (KB) netýkala. Svet OT bol pre bežný svet informačných technológií (IT) veľkou neznámou; svet, v ktorom žili špecialisti, ktorým len málokto rozumel. Iba nemnoho spoločností investovalo prostriedky na ochranu OT pred kybernetickými incidentmi. Kľúčovým zlomom rýchleho zblížovania svetov OT a IT bolo implementovanie technických prostriedkov z oblasti IT (počítače a operačné systémy, komunikačné protokoly, sieťové prvky atď.) do OT. Odvtedy sa svet OT otvoril širokej verejnosti a riziko kybernetického incidentu sa mnohonásobne zvýšilo. V súčasnosti už nikoho neprekvapí správa v masmédiách o úspešnom kybernetickom útoku na priemyselný podnik, ktorého následky podnik riešil celé mesiace. Vzhľadom na tieto skutočnosti je dnes nevyhnutné, aby si priemyselné podniky začali koncepčne budovať systém, ktorý minimalizuje riziko kybernetického incidentu a zabezpečí kontinuitu výroby a dodávok služieb.

Systém riadenia priemyselnej kybernetickej bezpečnosti (Cyber Security Management System – CSMS) pokrýva celý životný cyklus KB, pričom je podporovaný normou ISA/IEC-62443. Na obrázku je zobrazený v praxi osvedčený CSMS, ktorý implementovali spoločnosti združujúce sa pod obchodnými značkami Actemium a Axians.

Zistiť

V prvom kroku implementácie CSMS sa v procese posudzovania skutkového stavu prostredníctvom osobných stretnutí so všetkými zainteresovanými osobami, podrobnou prehliadkou, inventarizáciou hardvéru a softvéru, workshopmi a pod. získavajú informácie, na základe ktorých sa skúma možný dosah kybernetických incidentov na podnik. Výsledkom tohto procesu je podrobná správa, ktorá okrem iného obsahuje aj maticu rizík s ohodnotením prijateľného rizika, odporúčania na zvýšenie odolnosti proti kybernetickým incidentom, ako aj logickú a fyzickú schému dátovej siete. Často sú už v tejto fáze identifikované nedostatky, takže možno okamžite aplikovať opatrenia, ako je napr. zmena segmentácie siete, modifikácia stratégie zálohovania, zaškolenie personálu alebo obmedzenie fyzického prístupu k vybraným zariadeniam.

Chrániť

Neoddeliteľnou súčasťou procesu ochrany je vzdelávanie zamestnancov o politike a postupoch z oblasti KB platných v podniku. Základným cieľom aplikovania technických opatrení v tomto procese je zmenšovanie priestoru, ktorý by mohol byť zneužitý na

kybernetický incident. Na to sa odporúča aplikovať postupy opísané v Guide to ICS Security 800-82 dostupné na internetových stránkach National Institute of Standard and Technology (NIST SP 800-82 rev. 2).

Odhalit'

Pre podnik je kľúčové vedieť identifikovať kybernetické incidenty včas. Vzhľadom na veľkú komplikovanosť systémov nasadených v podnikoch je vhodné, aby mal personál starajúci sa o kybernetickú bezpečnosť k dispozícii adekvátne technológie, ktoré nielen monitorujú kritické služby, sieťovú prevádzku, servery, pracovné stanice a pod., ale ktoré v reálnom čase analyzujú bezpečnostné výstrahy.

Reagovať

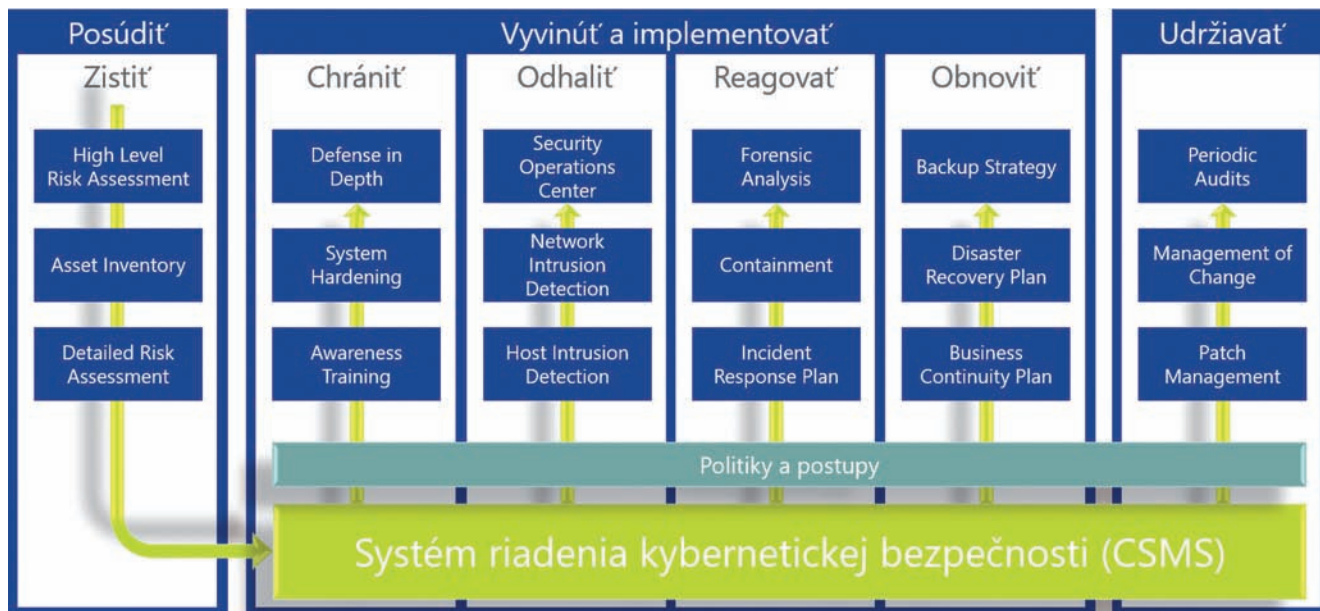
Správa hodnotenia rizík, ktorá bola vypracovaná v prvom kroku implementácie CSMS, obsahuje realistické scenáre ohrozenia, ktoré majú vplyv na najdôležitejšie procesy a aktíva podniku. Napriek prijatým opatreniam musí byť podnik pripravený na prípadný incident. Pre podnik je strategické mať vypracovaný akčný plán na identifikáciu a kontrolu kybernetického incidentu, ktorý zaistí včasnú a správnu reakciu. Každý kybernetický incident, ktorý bol v podniku identifikovaný, treba podrobne analyzovať. Výsledky forenzných analýz pomôžu lepšie porozumieť incidentu, ku ktorému došlo, a upraviť procesy tak, aby sa podobný bezpečnostný incident neopakoval.

Obnoviť

Pre podnik je štandardom mať vypracované plány kontinuity a obnovy s cieľom pokračovať v najdôležitejších obchodných procesoch v rôznych scenároch. V súčasnosti je dôležité, aby boli súčasťou týchto plánov aj procesy týkajúce sa KB, nakoľko závislosť podniku od OT a IT mu neumožňuje tieto procesy podceňovať. Rýchlosť obnovy systémov po kybernetickom incidente je pre podnik kritická. Efektívna stratégia zálohovania systémovej platformy, aplikačného softvéru a kmeňových výrobných údajov následne podniku umožňujú rýchlu obnovu výroby a dodávok služieb.

Udržiavať

Implementácia CSMS nie je jednorazovým projektom, ale je systémom, ktorý vyžaduje neustálu pozornosť. OT a IT sú predmetom neustálych zmien nielen z dôvodu rozširovania alebo realizácie technologických zmien, ale aj z dôvodu aplikovania zmien organizačných



a personálnych. Pre podnik je dôležité pravidelne kontrolovať, či sú implementované politiky, postupy a opatrenia stále účinné. Každá aplikovaná zmena je potenciálnym rizikom a z uvedeného dôvodu norma ISA/IEC-62443 vyžaduje povinné zavedenie systému riadenia zmien.

Vnímame rozdiely medzi stavom pripravenosti podnikov na prípadné bezpečnostné incidenty. V zahraničí sa spoločnosti snažia už dlhšie o systémové riešenia, na Slovensku však podniky ešte len nasadzujú technologické opatrenia. Často hlavným (a nezriedka jediným) dôvodom, prečo sa podniky začali problematike priemyselnej kybernetickej bezpečnosti venovať, je nadobudnutie účinnosti zákona o kybernetickej bezpečnosti č. 69/2018 Z. z.

Skúsenosti z nasadzovania KB v praxi slovenských podnikov

Na rozdiel od zahraničných kolegov zo skupiny Actemium spoločnosť ProCS (Actemium Slovakia) zatiaľ neimplementovala komplexný CSMS. V praxi sme sa stretli so zákazníkmi, ktorí sa už vo svojich technických požiadavkách venujú problematike KB a požadujú, aby bol dodávaný projekt v súlade s ich bezpečnostnou politikou.

Nedávno spoločnosť ProCS realizovala projekt, v ktorom zákazník venoval KB rovnakú mieru dôležitosti ako ktorejkoľvek inej časti projektu. V prvej fáze uvedeného projektu sa riešila sieťová KB. Tú zákazník považoval za kľúčovú, nakoľko striktné nastavenie komunikačných pravidiel na aktívnych sieťových zariadeniach mu pomohlo značne obmedziť možnosti kybernetického incidentu. Pre projekt bol vyhradený rozsah siete, ktorý bol rozdelený na virtuálne podsiete. Rozhodnutím využiť virtuálne podsiete sa v tomto prípade docielilo výraznejšie zvýšenie odolnosti celej sieťovej infraštruktúry v OT. Medzi jednotlivými virtuálnymi podsietami boli na základe použitých typov komunikačných protokolov nakonfigurované pravidlá ACL (Access Control List), ktoré zabezpečovali filtrovanie sieťovej prevádzky. Zlaté pravidlo „všetka komunikácia je štandardne zakázaná“ bolo použité pri konfiguráciách všetkých aktívnych sieťových zariadení. Pravidlá ACL boli nastavované v súlade s odporúčením výrobcov OT a IT, použitých komunikačných protokolov a výsledkov analýzy sieťovej prevádzky. Všetky komunikačné protokoly použité v projekte museli spĺňať podmienku šifrovania. Na záver sa zrealizovali základné penetračné testy, ktoré potvrdili správnosť nastavenia všetkých aktívnych sieťových prvkov dátovej siete.

Bezpečná pripojiteľnosť vybraných používateľov zo zóny IT na server umiestnený vo vyhradenej zóne OT bola ďalšou úlohou, ktorú bolo nevyhnutné vyriešiť. Štandardne dodávaný klient na komunikáciu so serverom nespĺňal bezpečnostné požiadavky zákazníka a bolo potrebné nájsť riešenie, ktoré by používalo predpísaný komunikačný

protokol. Rozhodnutie použiť protokol RDP znamenalo obmedziť prostredie pre vzdialených používateľov na serveri tak, aby mali možnosť používať iba vybrané aplikácie bez možnosti akejkoľvek inej interakcie alebo zásahu do funkčnosti servera.

Použité operačné systémy na serveroch a operátorských pracoviskách v predvolenom nastavení nereflektovali požiadavky konkrétnej implementácie a bolo nutné vykonať hardening (spôsob modifikácie nastavení parametrov zariadenia tak, aby bolo čo najviac optimalizované na jeden konkrétny účel). Vzhľadom na nasadené technológie bolo potrebné vykonať veľké množstvo nastavení a testov. Výsledkom tohto procesu bola optimalizácia výkonu zariadení, zvýšenie odolnosti proti kybernetickým hrozbám a zníženie počtu porúch vzniknutých nevyužívanými službami.

KB bola súčasťou akceptačných testov FAT a SAT, na ktorých sa overoval súlad nastavení, funkčnosti a výkonu s požiadavkami. Okrem uvedených služieb sa zákazníkovi vypracovala projektová dokumentácia KB, ktorá obsahovala detailný opis sieťovej infraštruktúry, nastavenie pravidiel ACL, opis komunikácie medzi IT a OT, nastavenie auditovania a logovania, opis fyzickej ochrany, stratégiu zálohovania, nastavenie parametrov hardeningu, podrobný zoznam hardvérovej a softvérovej inventarizácie, nastavenie bezpečnostných politík, konfiguráciu sieťových zariadení, zoznam hesiel a nastavenie firewallov. Všetky citlivé informácie boli odovzdané v šifrovanej forme. Na záver bol technický personál zákazníka zaškolený do KB.

Úspešné nasadenie KB je o úzkej spolupráci

Spoločnosti, ktoré dodávajú komplexné riešenia pre priemyslú automatizáciu, musia rozširovať svoje kompetencie o oblasť priemyselnej kybernetickej bezpečnosti, aby boli pripravené čeliť novej výzve a dodávať produkty a služby, ktoré budú zapadať do koncepcie CSMS zákazníka. Prvé naše skúsenosti so zákazníkmi z energetického a chemického priemyslu na Slovensku nám ukázali, že zvládnuť tento proces nie je triviálne. Je potrebné, aby veľmi úzko spolupracovali špecialisti z oblasti OT a IT na strane dodávateľa aj na strane zákazníka.



ProCS, s.r.o.

Kráľovská ulica 8
927 01 Šaľa
Tel.: +421 31 7731 111
info@actemium.sk
www.actemium.sk

RIEŠENIA KYBERNETICKEJ BEZPEČNOSTI END-TO-END PRE AUTOMATIZÁCIU

Kybernetická bezpečnosť nepredstavuje jedno riešenie jedného problému, predstavuje skôr neustály súboj, ktorý vyžaduje viacero prístupov a riešení – v záujme komplexnosti a systémového prístupu však najlepšie z jedného zdroja s bohatými skúsenosťami a so širokým portfóliom riešení v špecifickej oblasti digitalizovaného priemyslu. Líder v inováciach technológií spoločnosť ABB, má vo svojom portfóliu rad takýchto produktov.

Súlada s medzinárodnými normami kybernetickej bezpečnosti

Pre automatizačné systémy súčasnosti je charakteristické spájanie s viacerými sieťami, systémami, miestami. Dosahujú tak výrazne vyššiu účinnosť prevádzky. Na druhej strane však tento proces prináša otázky týkajúce sa kybernetickej bezpečnosti, ktoré boli dotiaľ známe len pre kancelárske alebo podnikové IT systémy. Riešenia kybernetickej bezpečnosti end-to-end spoločnosti ABB čelia rizikám, ktoré sa môžu vyskytnúť kdekoľvek – od riadiacich centier, cez komunikačné siete až po automatizáciu rozvodní.

Spoločnosť je lídrom digitalizácie v priemysle a definuje jej štandardy

Špecialisti spoločnosti vyvíjajú vysoko bezpečné, dôveryhodné riešenia kybernetickej bezpečnosti pre celú oblasť priemyselnej automatizácie, jej infraštruktúru alebo kritické aplikácie. V rámci životného cyklu všetkých výrobkov ABB sa uvažuje s kybernetickou bezpečnosťou, ktorá sa riadi osvedčenými postupmi opísanými v normách IEC 62443, IEC 62351, NERC-CIP, IEEE 1686, ako aj odporúčaniami BDEW. Spoločnosť ABB je aktívnym členom viacerých priemyselných iniciatív týkajúcich sa kybernetickej bezpečnosti vrátane organizácií IEEE a IEC. Podieľa sa v nich na tvorbe noriem, sleduje potreby svojich zákazníkov a následne ich transformuje do nových noriem a odporúčaní.

Prístup Defense in depth

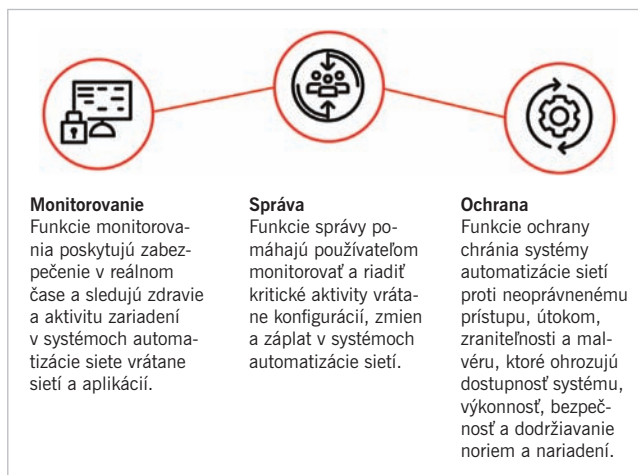
Opatrenia kybernetickej bezpečnosti pomáhajú monitorovať, riadiť a chrániť systémy a produkty, aby boli v súlade s priemyselnými normami a s prístupom Defense in depth. Všetky systémy automatizácie siete od ABB sú navrhnuté a nakonfigurované podľa osvedčených postupov a poskytujú širokú škálu opatrení kybernetickej bezpečnosti. Zoskupené sú do troch hlavných kategórií (obr. 1).

Riešenia kybernetickej bezpečnosti end-to-end

Riešenia ABB zaisťujú bezpečnosť systému a zariadení z riadiaceho centra na sieťovej úrovni cez komunikačnú až po procesnú úroveň. Bezpečnostné úrovne podľa IEC 62443.

Ponuka riešení kybernetickej bezpečnosti

Pridaním niekoľkých vrstiev riadenia bezpečnosti naprieč systémom možno vybudovať bezpečný systém v súlade s Defense in depth.



Obr. 1

Skupiny funkcií kybernetickej bezpečnosti z portfólia ABB pomôžu zabezpečiť všetky priemyselné systémy na špičkovej úrovni.

Bezpečná komunikácia

Naše riešenia používajú najnovšie šifrovacie technológie podľa normy IEC 62351. Príkladmi sú https, tunelovanie VPN pre vzdialený prístup, bezpečná IEC 60870-5-104 a bezpečná komunikácia DNP 3.0 v súlade s IEC 62351. Okrem toho ABB využíva riešenia Quantum-Safe na vysoko bezpečné šifrovanie end-to-end a dlhodobú ochranu v kriticky dôležitých komunikačných sieťach.

Zónovanie a ochrana perimetra

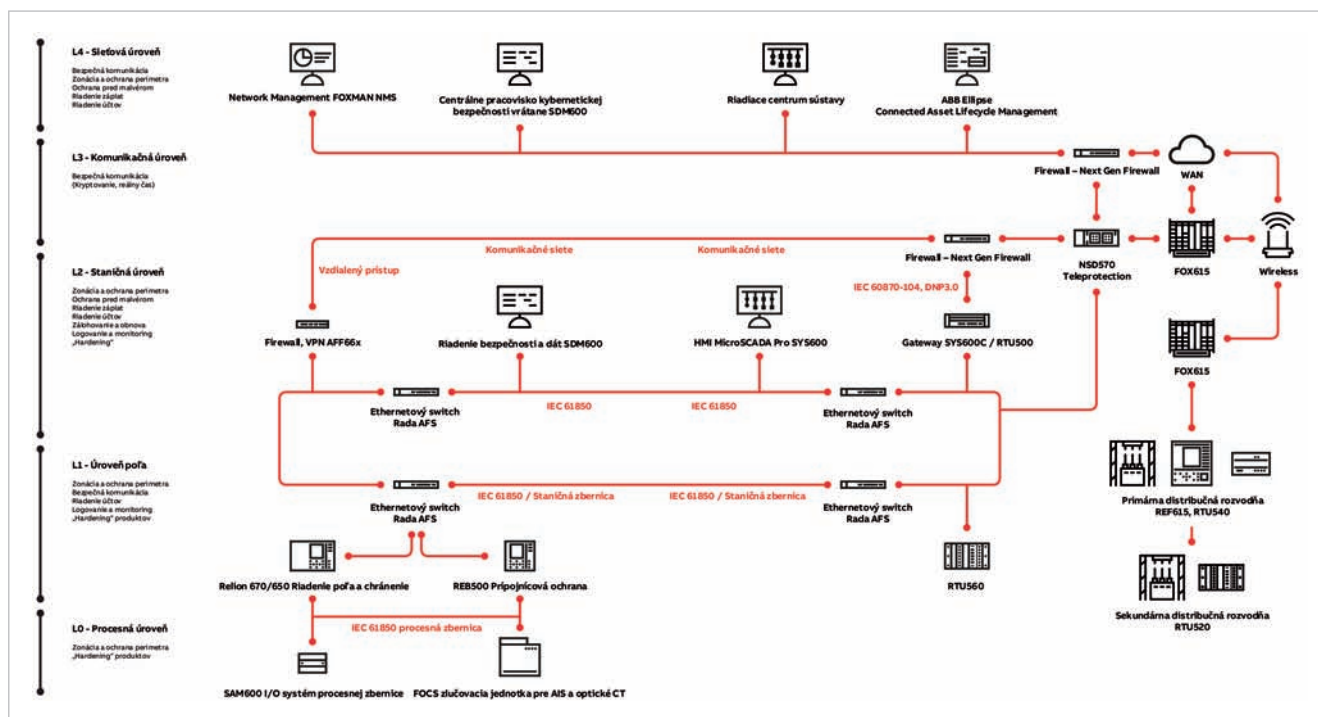
Firewally chránia perimeter siete, rozdeľujú ich do bezpečnostných (demilitarizovaných) zón, čím sa zaisťuje, že postihnutý systém neohrozí celú sieť. Na podrobnejšiu kontrolu sa môžu zahrnúť firewally novej generácie (NGFW – Next Generation Firewall) vrátane systému detekcie prieniku (IDS – Intrusion Detection System) na zlepšenie schopnosti monitorovania a ochrany.

Ochrana pred malvérom

Riešenia ochrany pred malvérom a neoprávneným vniknutím chránia siete pred vírusmi, trójskymi koňmi a inými typmi malvéru. Okrem toho možno pridať riešenie na ochranu pred spustením neoprávnených aplikácií.

Norma	Hlavné zameranie
NERC CIP	Nariadenie o kybernetickej bezpečnosti pre distribučné spoločnosti v Severnej Amerike
IEC 62351*	Bezpečnosť dát a komunikácie
IEEE 1686	Norma IEEE týkajúca sa vlastností kybernetickej bezpečnosti inteligentných elektronických zariadení (IED) na rozvodniach
IEC 62443*	Priemyselná automatizácia a zabezpečenie riadiacich systémov (predtým ISA S99)
BDEW Whitepaper	Požiadavky na bezpečné riadenie a telekomunikačné systémy

* Štandardy stále v príprave



Obr. 2

Riadenie záplat

Riadenie záplat (Patch management) je jednou z najdôležitejších vrstiev kybernetickej bezpečnosti v digitálnych systémoch. Na zaistenie vysokej bezpečnosti počas celého životného cyklu systému poskytuje ABB komplexné riešenia na riadenie záplat.



Zálohovanie a obnova

ABB ponúka kompletné zálohovania ako opatrenie pred neželanou stratou dát, zlyhaním hardvéru a softvéru a kybernetickými útokmi, ktoré umožňujú používateľom byť vždy pripravený na najhoršie.



Riadenie účtov

Systémy ABB poskytujú rozsiahle možnosti riadenia používateľských účtov v súlade s rolami a oprávneniami. Na správu veľkého množstva zariadení ponúkame centrálnu riešenie na správu používateľských účtov založené na IEC 62351-8, v ktorom používateľ definuje zložitosť hesla. Pri vzdialenom prístupe možno použiť dvojfaktorové overenie.



Loggovanie a monitorovanie

Vytvárajú sa podrobné auditorské trasy (súbory logov) všetkých používateľských aktivít súvisiacich s bezpečnosťou. Tieto možno poslať do centrálnu systému riadenia na ďalšiu analýzu. Umožňuje zákazníkom sledovať bezpečnostné udalosti v reálnom čase a reagovať na ne.



Hardening produktov a systémov

Všetky produkty ABB sú úspešne overené v nezávislom centre zaručenia bezpečnosti zariadenia (DSAC – Device Security Assurance Center). Vo fáze inžinieringu a testovania bude dodaný systém posilnený v zmysle známych osvedčených postupov.



Kybernetická bezpečnosť počas životného cyklu systému

V ABB sa kybernetická bezpečnosť rieši vo všetkých fázach životného cyklu navrhovaného systému. Zohľadňuje sa pri návrhu, vývoji aj prevádzke a údržbe. Potreby kybernetickej bezpečnosti vo všetkých fázach procesu vývoja sa zaoberá program SDL (Security Development Lifecycle).

Modelovanie hrozieb a revidovanie bezpečnostných návrhov, bezpečnostné školenia pre vývojárov softvéru a externé bezpečnostné

testovanie sú iba niektoré z mnohých činností, ktoré ABB vykonáva, aby zákazníkom poskytla spoľahlivé a bezpečné riešenia. Individuálne používateľské kontá a podrobné denníky bezpečnostných udalostí sú len dva príklady zabudovaných bezpečnostných funkcií dostupných v našich produktoch.

Kľúčovou črtou ponuky ABB je nezávislé centrum zabezpečenia zariadení (DSAC). Pred uvoľnením na trh sa v ňom všetky produkty ABB podrobujú najmodernejšiemu bezpečnostnému testovaniu.

Quantum-Safe – riešenia pre kritickú komunikáciu

Rastúca hrozba kybernetických útokov na kritické infraštruktúry, ako sú elektrické siete a nové vektory hrozieb ako kvantový počítač, znamená, že tieto siete nevyhnutne potrebujú lepšiu ochranu. ABB ponúka prvé priemyselné riešenie Quantum-Safe na vysoko bezpečné šifrovanie MPLS-TP end-to-end, ktoré zohľadňuje špecifické potreby kritických aplikácií z hľadiska komunikačnej výkonnosti (napr. jitter, wander, latency), pričom berie do úvahy dostupnosť a dlhodobú ochranu komunikačnej infraštruktúry. Kvantové technológie zvyšujú celkovú bezpečnosť kritickej infraštruktúry zlepšením generovania kryptografických kľúčov prostredníctvom kvantového generátora náhodných čísel (QRNG – Quantum Random Number Generators).

ABB neustále rozširuje a aktualizuje bezpečnostné procesy, aby sa zraniteľnosť mohla riešiť rýchlo a správne. Včasná reakcia je nevyhnutná na to, aby pomohla zákazníkom minimalizovať vystavenie sa hrozbám kybernetickej bezpečnosti. Všetky zistenia sa môžu hlásiť neformálne prostredníctvom e-mailu.

Okrem technických riešení môže ABB poskytovať školenia, poradenstvo a riešenia na posudzovanie rizík kybernetickej bezpečnosti. Hodnotenie poskytuje technickú aj organizačnú analýzu a navrhuje optimalizované opatrenia na zníženie rizík kybernetickej bezpečnosti.



Ján Lukačín

ABB, s.r.o.
Tuhovská 29
831 06 Bratislava
www.abb.sk

VOĽNE PROGRAMOVATEĽNÝ IZBOVÝ REGULÁTOR SBC PRE PRUŽNÉ A INDIVIDUÁLNE APLIKÁCIE



Od optimalizácie spotreby energií po vytváranie unikátneho používateľsky príjemného prostredia, programovateľné regulátory SBC umožňujú osloviť skupinu zákazníkov so špecifickými požiadavkami na automatizáciu budov v hoteloch, nemocniciach a kanceláriách. S novým IRM voľne programovateľným regulátorom Saia PCD7.LRLxx-P5 možno vytvárať na mieru aplikácie na riadenie vykurovania, chladenia, vzduchotechniky, osvetlenia a tienenia.

Na pokrytie špecifických potrieb daného prostredia je ľahké doplniť ďalšie senzory a funkcie. To zahŕňa napríklad moduly DALI, detektory pohybu alebo hotelové čítačky kariet. Vďaka vysokej úrovni pružnosti možno vytvárať scény, ktoré ponúkajú hosťom a návštevníkom unikátnu skúsenosť zdôrazňujúcu napr. individualitu konceptu a prostredie hotela.

Jeden nástroj – veľa možností

Programovanie sa vykonáva prostredníctvom Saia PG5 Controls Suite a do regulátora sa program nahrá cez pripojenie USB. Izbový regulátor môže byť použitý aj v kombinácii s komplexným projektom PG5, vrátane iných produktov SaiaPCD, ktoré sú súčasťou celkového riešenia. To znamená, že jediný softvérový nástroj môže byť použitý na realizáciu rôznych požiadaviek od riadenia priestoru až po správu budov či na efektívne a jednoduché programovanie. Používanie rôznych softvérových riešení alebo dodatočného hardvéru nie je nutné.

Päť verzií s ohľadom na rôzne požiadavky

Voľne programovateľný izbový regulátor SBC sa vyrába v dvoch malých a troch veľkých variantoch. S rôznou konfiguráciou I/O sa regulátor vie prispôsobiť zodpovedajúcim okolnostiam a potrebám. Univerzálne analógové a binárne vstupy ponúkajú pružnosť na integráciu individuálne riešených objektov. Dve komunikačné rozhrania môžu byť nakonfigurované na komunikáciu cez S-Bus alebo Modbus, čo umožňuje pripojenie do nadradeného riadiaceho systému budov, rovnako ako integráciu digitálnych izbových ovládačov alebo rozširovacích modulov zo sortimentu SBC E-Line. Pre prípad rekonštrukcie objektu je veľmi jednoduché implementovať

bezdrôtové senzory a pohony EnOcean. V neposlednom rade možno k regulátorom pripojiť izbové nástenné ovládače s komunikáciou SYLKbus so zabudovanými senzormi teploty, vlhkosti alebo CO₂. Regulátory sú vhodné najmä na riadenie prostredia v miestnostiach s najvyššou energetickou účinnosťou. Sú vybavené vysoko kvalitnými testovanými a overenými konfigurovateľnými aplikáciami na riadenie:

- 2- a 4-rúrkového FCU,
- 1 až 3-stupňového ventilátora, ventilátora s premenlivou rýchlosťou,
- nasávaného vzduchu s kontrolou kvality vzduchu,
- chladiaceho stropu,
- podlahového vykurovania,
- radiátorového vykurovania,
- kombinácií vyššie uvedených aplikácií.

Aby sa dosiahla maximálna energetická účinnosť, aplikácie podporujú regulačné a šesťcestné ventily, ventilátory s premenlivou rýchlosťou, kontrolu kvality vzduchu v interiéri a ďalšie.

Ďalšie informácie nájdete na webových stránkach oficiálneho distribútora Saia Burgess Controls pre Českú republiku a Slovensko spoločnosti EWWH, spol. s r. o.

EWWH
Komponenty pro automatizaci řešení

EWWH, s.r.o.

Hornoměřcholupská 68
102 00 Praha 10
Tel.: +420 734 823 339
obchod@ewwh.cz
www.ewwh.sk

PHOENIX CONTACT PREDSTAVUJE PROGRAMOVATEĽNÝ SYSTÉM LOGICKÝCH RELÉ PLC logic

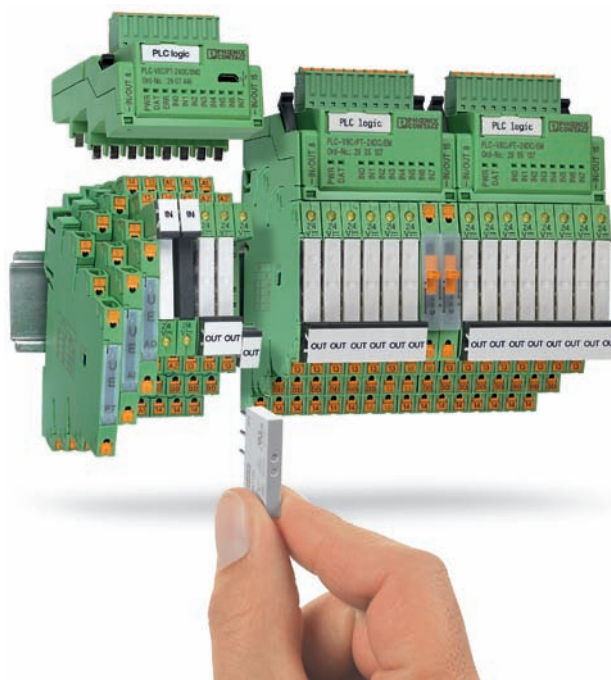
Tak ako sa čoraz častejšie vyžadujú menšie rozmery a vyššia inteligencia zariadení, zabudúva sa do programovateľných logických reléových systémov logika.

Do štandardného rozhrania sa jednoducho pripojí PLC ako kompaktný malý kontrolér. Šesťnásť V/V modulov s celkovou šírkou len 50 mm riadi automatizačné úlohy na najmenšom možnom priestore. Osem V/V možno zvoliť ľubovoľne – či už pre digitálne, alebo analógové signály, vstup alebo výstup. Základné moduly možno rozšíriť dvomi rozširovacími modulmi, vďaka čomu možno dokopy načítať a spínať 48 V/V signálov. Ak je niektoré z relé na konci svojej životnosti, používateľ ich dokáže vymeniť za pár sekúnd, a to bez nutnosti vymieňať celú riadiacu jednotku. Na požiadanie možno efektívne urobiť aj káblovanie PLC logiky, a to vďaka zásuvnej (push-in) technológii. Pre tento prípad sa do upínacej časti pripoja pevné vodiče a vodiče s konektormi, navyše bez potreby náradia. Intuitívne ovládanie softvéru Logic+ umožňuje rýchle naprogramovanie logického reléového systému, ktoré zvládne aj elektrotechnik bez špeciálneho zaškolenia. Na to, aby to zvládol, potrebuje len základnú znalosť elektrických obvodov a digitálnej technológie.

Programovacie jazyky ako rebríkové diagramy (LD) a diagramy funkčných blokov (FBD) sa napríklad vytvárajú spôsobom „zober a polož“ konkrétnych funkčných blokov a ich prepojení. Celý program možno následne simulovať a otestovať offline aj online.

Jednoduchú prevádzku podporuje aj reprezentácia PLC logiky v hardvérovom editore. Rozsah služieb zahŕňa aj bezdrôtový prístup k prevádzkovým údajom cez Bluetooth prostredníctvom aplikácie PLC logiky inštalovanej na inteligentnom zariadení, ako aj cez voliteľné prispôsobiteľné brány pre bežné zbernicové systémy.

Reléový systém s logikou možno rýchlo a pohodlne využiť v prípade vzdialene rozmiestnených alebo z hľadiska funkcionality



podriadených riadiacich jednotiek. Rozsah aplikácií siaha od automatizácie budov, ako je napr. riadenie žalúzií, ventilácie a osvetlenia v podzemných garážach, až po decentralizované strojné zariadenia alebo systémové prvky v rámci výrobných automatizácií.

Výhody PLC logic

- vysoká dostupnosť vďaka zásuvným spínacím prvkom,
- flexibilné kombinovanie: osadíte každý kanál individuálne ako vstup alebo výstup reléovými alebo analógovými modulmi podľa požiadavky danej aplikácie,
- efektívne prepojenie vďaka technike pripojenia push-in a špeciálnym variantom na prepojenie senzorov,
- jednoduchá realizácia projektov vďaka intuitívnemu softvéru Logic+,
- bezdrôtové ovládanie a dohľad pomocou adaptéra Bluetooth a aplikácie PLC logic,
- programovateľný systém logických relé je súčasťou systému COMPLETE line.

Ján Kadlečík

PHOENIX CONTACT, s.r.o.
Námestie Mateja Korvína 1
811 07 Bratislava
Tel.: +421 2 3210 1470
obchod.sk@phoenixcontact.com
www.phoenixcontact.sk



ZMEŇME VÝROBU Z AUTOMATIZOVANEJ NA AUTONÓMNU



Výroba budúcnosti bude založená na cyber-fyzikálnych, autonómnych a samoučiacich sa systémoch. Autonómne stroje a roboty sa dokážu učiť a rozoznávať pracovné prostredie.

V definovanom rozsahu sa budú prispôbovať meniacim sa okolitým podmienkam a požiadavkám a budú sa autonómne rozhodovať. Toto je možné vďaka IT technológiám založeným na umelej inteligencii, rozšírenej realite a edge computingu.

Umelá inteligencia je kľúčovým faktorom k zvyšovaniu produktivity výrobných automatizovaných systémov. Umelá inteligencia umožní vykonávať strojom prácu, ktorú doteraz musel vykonávať iba človek. Vďaka tomu dokážu výrobcovia strojov zvýšiť efektivitu a optimalizovať jednotlivé operácie. Príkladom môže byť vizuálna kontrola kvality, analýza kvality na základe digitálnych modelov (dvojičiek), autonómna manipulácia a transport zvýši flexibilitu vo výrobe a detekcia anomálií a condition monitoring vytvorí základ pre preventívnu údržbu a zabráni neželaným prestojom.

V budúcnosti môže rozšírená realita kompletne zmeniť výrobné procesy a vývoj produktov. Toto bude možné vďaka digitálnemu obrazu produktov a informáciám premietnutým do reálneho prostredia výroby. Flexibilita a efektivita manuálnych činností môže byť zvýšená zobrazením inštrukcií krok za krokom v prostriedkoch rozšírenej reality priamo počas výrobných operácií na výrobných linkách.

Edge computing sa stáva kľúčovým nástrojom na zber, analýzu a management výrobných dát v lokálnych sieťach. Vďaka veľkému výpočtovému výkonu je možné časť výpočtových úloh (vrátane umelej inteligencie, neurónových sietí,...) spracovať priamo na stroji a efektívne využívať najpokročilejšie

metódy spracovania dát bežiacich v cloud. Toto dáva možnosť na efektívnu distribúciu algoritmov umelej inteligencie podľa potrieb aplikácie. Veľkou výhodou edge computing je možnosť updatovať a modifikovať lokálne bežiace aplikácie vzdialene (aj hromadne z cloudu).

Siemens pracuje na škálovateľnom a veľmi dobre prispôbitelnom riešení aplikácie umelej inteligencie v každej časti TIA portfólia, čo umožňuje našim zákazníkom získať značnú konkurenčnú výhodu do budúcnosti.

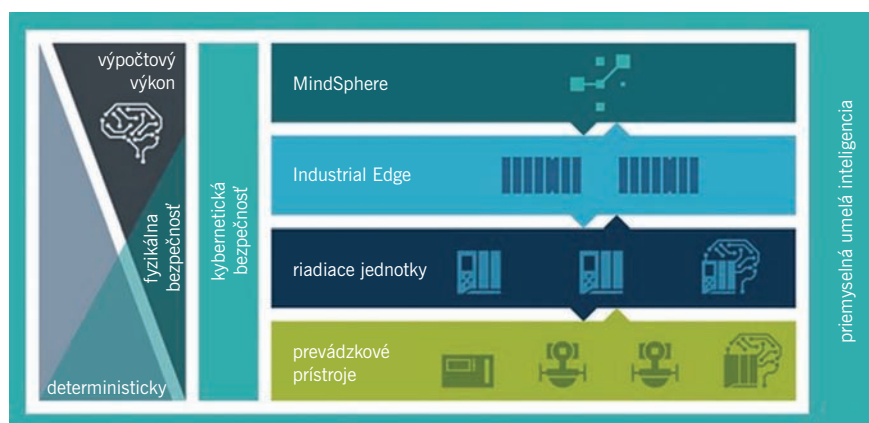
Umelá inteligencia v systéme SIMATIC

Umelá inteligencia (UI) bude najmä v priemysle rozhodujúcou mierou prispievať k redukcii nákladov na programovanie a inžiniersku činnosť pri riešení úloh automatizácie.



Budúcnosť automatizácie

Umožňuje vytvárať logické riadenie na báze strojového učenia a výrobné procesy s vyššou flexibilitou a presnosťou. Napríklad systémy vizuálnej kontroly kvality alebo priemyselné roboty navádzané na základe rozpoznávania obrazu reagujú s využitím algoritmov strojového učenia výrazne



Obr. 1

flexibilnejšie na nepredvídané situácie alebo na identifikované nedostatky v kvalite produktov, a to automaticky v reálnom čase počas prevádzky. Vďaka expertným znalostiam algoritmy prenesené do riadiacich systémov pracujú podstatne efektívnejšie, napríklad čo sa týka farby, zloženia alebo kvality produktu alebo procesu do systému automatického riadenia.

Umelá inteligencia vytvára nové možnosti

Umelá inteligencia umožňuje riešiť také úlohy automatizácie, pri ktorých sa klasické metódy riešenia dostávajú na svoje obmedzenia. Postupne sa etabluje na všetkých úrovniach portfólia Totally Integrated Automation (TIA) – od úrovne prevádzky až po cloud.

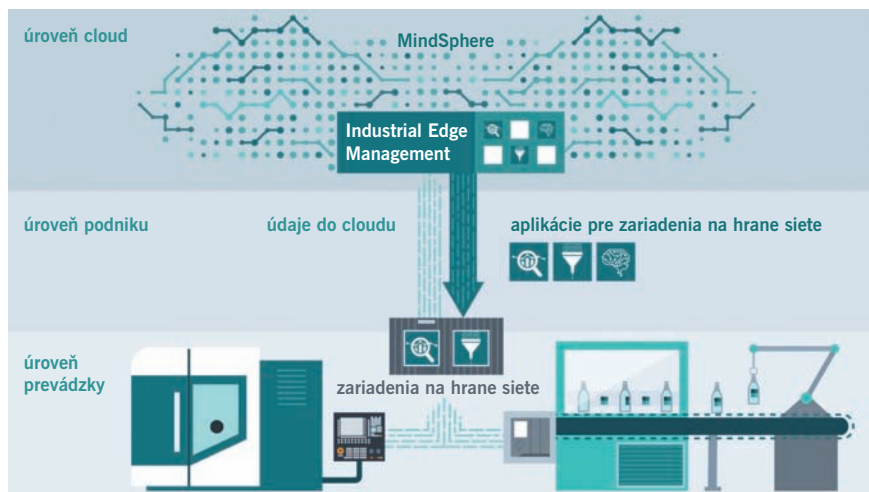
Umelá inteligencia (UI) a Totally Integrated Automation (TIA)

UI bude tvoriť dôležitý prvok v budúcnosti automatizácie. V rámci Totally Integrated Automation (TIA) sa uplatní od najmenších riešení na úrovni snímačov a akčných členov cez edge zariadenia až na úroveň cloudu, vďaka podpore IoT operačného systému MindSphere je to možné už dnes. Tak sa môže riešenie na báze umelej inteligencie využiť pre jeden stroj, celú výrobnú linku alebo celý výrobný závod.

Prvým dôležitým krokom k integrácii umelej inteligencie do prostredia automatizácie je nový modul S7-1500 TM NPU. Je špeciálne vhodný na inštaláciu do rozvádzačov strojov – všade tam, kde sa požadujú spoľahlivé, rýchle a deterministické rozhodnutia.

Nový modul SIMATIC S7-1500 TM NPU

S novým modulom S7-1500 TM NPU (Neural Processing Unit) pre riadiaci systém SIMATIC S7-1500 a I/O- systém ET 200MP vstupuje umelá inteligencia prostredníctvom systému TIA do automatizácie. Modul sa bezproblémovo integruje do riadiaceho systému SIMATIC a tým umožňuje jednoduchú a efektívnu kombináciu algoritmov umelej inteligencie a logických funkcií programovateľných logických automatov. To umožňuje cenovo efektívne realizovať na úrovni stroja v systéme SIMATIC úlohy



Obr. 3

na báze umelej inteligencie. Modul S7-1500 TM NPU je vybavený procesorom pre spracovanie úloh umelej inteligencie »Myriad™ X Vision Processing Unit« od Intel Movidius™, ktorý sa okrem iného vyznačuje efektívnym vykonávaním funkcií neurónových sietí.

Modul TM NPU môže byť inštalovaný centralizovane za procesorom S7-1500 ako aj decentralizovane v systéme ET 200MP. Zasunutím viacerých modulov za sebou možno okrem toho riešenie podľa potreby prispôbiť veľkosti štruktúry a počtu realizovateľných aplikácií.

Modul S7-1500 TM NPU obsahuje SD kartu s natrénovanou neurónovou sieťou, ktorú vykonáva. Na integrované rozhrania modulu môžu používatelia pripojiť senzory prostredníctvom gigabitového Ethernetu a USB3.1 ako napr. kamery alebo mikrofóny. Ako vstupné dáta možno použiť aj dáta z PLC, prenášané cez jej zadnú zbernicu (backplane). Výsledky výpočtu sa potom vyhodnocujú v programe PLC procesora.

Edge computing prináša novú slobodu

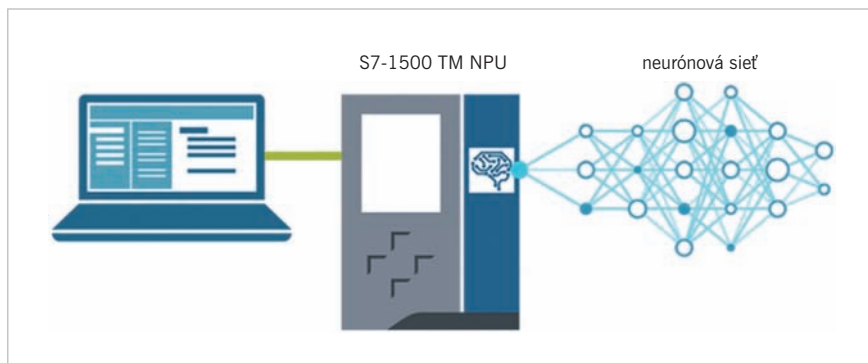
Inovačné cykly sú stále kratšie a kratšie, systémy a spoločnosti sú stále viac prepojené. Efekty digitalizácie sú stále zreteľnejšie. Firmy, ktoré chcú zostať konkurencie schopné, musia byť pripravené flexibilne reagovať na zmeny. Dodatočne k ich hlavným výrobným úlohám budú musieť hľadať efektívne

a lacné riešenia ako modernizovať výrobné procesy a zabezpečiť IT bezpečnosť.

Lokálne alebo centrálnne, v lokálnej sieti alebo cez internet, na vlastnej infraštruktúre alebo ako servis – firmy majú rôzne možnosti ako zbierať a analyzovať výrobné dáta a trvalo zlepšovať svoje procesy. Mnoho spoločností upúšťa od lokálneho spracovania dát na vlastnom hardvérovom vybavení a spoliehajú sa na cloudové riešenia. To im umožňuje jednoducho updatovať a manažovať aplikácie. Pri tomto prístupe je nutné predspracovať dáta lokálne a prenášať do cloudu už predspracovanú informáciu. Siemens Industrial Edge ekosystém je kombináciou hardvéru a softvéru, ktorá efektívne rieši problém bezpečného a spoľahlivého predspracovania dát. Edge zariadenia a edge aplikácie je možné centrálnne spravovať a tiež distribuovať na novo pripojené stroje. Systém tiež umožňuje jednoduchú distribúciu updatov a bezpečnostných opráv, čo pripravuje stroje na budúcnosť.

Simatic IPC227E Edge Device

Simatic IPC227E Edge Device je extrémne kompaktný a flexibilný embedded priemyselný počítač. So svojou uzavretou celokovovou konštrukciou Simatic IPC 227E ponúka maximálnu priemyselnú odolnosť aj v tých najnáročnejších aplikáciách a spoľahlivú bezúdržbovú prevádzku. Toto tvorí ideálnu platformu pre priemyselné edge aplikácie. Edge softvér je už predinštalovaný, čo zrychľuje uvedenie do prevádzky. Súčasťou sú komunikačné rozhrania pre riadiace systémy a pre cloud, ako aj výkonne prostredie pre beh edge aplikácií.



Obr. 2

SIEMENS
Ingenuity for life

Siemens s.r.o.

Lamačská cesta 3/A
841 04 Bratislava
www.siemens.sk

NOVÁ GENERÁCIA BECKHOFF IPC A UPS



Novú sériu ultrakompaktných priemyselných PC odštartovalo vydanie modelu C6015, ktorý sa stal vďaka svojim rozmerom len 82 x 82 x 40 mm a flexibilita veľmi úspešným na trhu, hlavne v oblasti IoT a Industry 4.0.

Okrem výborného pomeru cena a výkon tento model ponúka všetky štandardné vlastnosti, ktoré by ste od priemyselného PC čakali, ako je vysoký teplotný rozsah od 0 °C do 55 °C, kompatibilita EtherCAT a vysoká odolnosť proti vibráciám a otrasom. Je osadený procesorom Intel® Atom™, ktoré sú dostupné vo verziách s jedným, dvoma alebo štyrmi jadrami. Ide o procesory z radu Embedded, ktoré zaručujú zákazníkovi dlhodobú dostupnosť a životnosť zariadenia. Veľkosť pamäte RAM možno zvoliť 2 GB alebo 4 GB. Ako úložné médium sa použil disk M.2 SSD s technológiou 3D MLC a voliteľnou kapacitou od 30 GB do 160 GB. Medzi použitými rozhraniami nájdeme 2 x Gigabit Ethernet, 1 x USB 3.0, 1 x USB 2.0 a 1 x DisplayPort.

Model C6017 rozširuje C6015 o ďalšie rozhrania 2 x Gigabit Ethernet a 2 x USB 2.0 a o jednosekundovú UPS, ktorú možno použiť na zálohovanie perzistentných dát v systéme TwinCAT. Priemyselné PC C6017 je len o 26 mm širšie ako model C6015, pričom ostatné rozmery sú rovnaké. Kryt na oba modely je vyrobený zo zliatiny hliníka a zinku, pričom sa používa iba pasívne chladenie. S podporou technológie multicore sú tieto zariadenia vhodné pre výkonné automatizačné, vizualizačné a komunikačné aplikácie.

Ďalším modelom v novej generácii ultrakompaktných IPC je C6030 s rozmermi iba 129 x 133 x 76 mm. Tento model využíva procesory Intel® Core™ i-series šiestej a siedmej generácie, kde patrí napríklad aj Core™ i7 so štyrmi jadrami a taktovacou frekvenciou 3,6 GHz, vďaka čomu možno toto zariadenie použiť na riadenie komplexných automatizačných aplikácií vyžadujúcich extrémne krátky čas cyklu a prácu s veľkým množstvom dát. Pamäť RAM možno rozšíriť až



Nová generácia IPC C6015 (vpravo) a C6017 (vľavo)

na 32 GB. Ako úložné médium sa opäť použil disk M.2 SSD s technológiou 3D MLC a voliteľnou kapacitou od 40 GB do 160 GB, pričom možno použiť až dva SSD disky v jednom IPC v konfigurácii RAID 1 na bezpečnú zálohu vašich dát. Model C6030 ďalej obsahuje 4 x Gigabit Ethernet, 4 x USB 3.0 a 2 x DisplayPort.



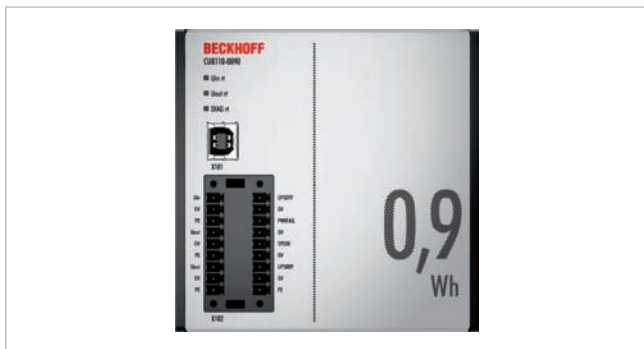
Nová generácia IPC C6030 (vpravo) a C6032 (vľavo)

Posledný model IPC uvedený firmou Beckhoff v tejto kategórii je C6032, ktorý rozširuje C6030 o dva prídavné moduly, kde možno vložiť rozširujúce rozhranie na Gigabit Ethernet, RS-232, USB 3.0 a CP-Link 4. Kryt na oba modely je opäť vyrobený zo zliatiny hliníka a zinku, ale bolo tu použité aktívne chladenie kvôli výkonným procesorom, ktoré sú osadené v C6030 a C6032.

Všetky priemyselné PC firmy Beckhoff sú určené na prácu s operačnými systémami Windows 7 a Windows 10 spoločnosti Microsoft.

Redizajnom v portfóliu spoločnosti Beckhoff prešli aj zariadenia UPS. K dispozícii je jeden typ kapacitnej UPS s kapacitou 0,9 Wh a dva typy batérie UPS s kapacitou 15 Wh a 30 Wh, pričom pri batériových UPS možno vymeniť samotnú batériu.





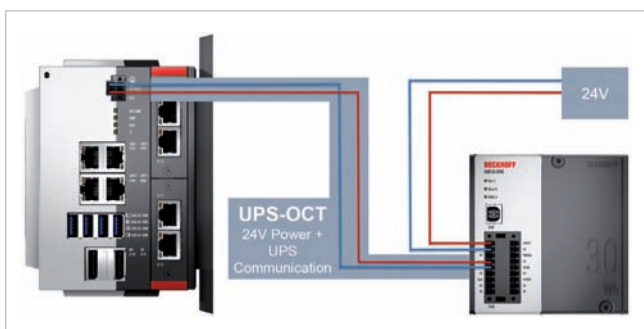
Kapacitná UPS CU8110-0090 s kapacitou 0,9 Wh



Batériová UPS CU8130-0090 s kapacitou 15 Wh a CU8130-0240 s kapacitou 30 Wh

Nový koncept umožňuje pripojiť UPS tromi rôznymi spôsobmi:

- OCT – One cable technology je technológia, ktorá umožňuje pripojiť UPS len pomocou jedného kábla, ktorým sa napája samotné IPC, ale zároveň po ňom prebieha komunikácia medzi UPS a IPC. Táto technológia bude dostupná pri nových typoch IPC spoločnosti Beckhoff, akým je napríklad model C6032.
- Digitálne I/O – UPS disponuje digitálnymi vstupmi a výstupmi, ktoré možno konfigurovať a pomocou nich signalizovať aktuálny stav UPS.
- USB – informácie o aktuálnom stave sa posielajú cez rozhranie USB.



Prepojenie OCT novej generácie UPS a IPC

Ak vás spomínané produkty zaujali, viac informácií o nich môžete nájsť na www.beckhoff.cz, prípadne sa môžete obrátiť na pracovníkov pobočky firmy pre Českú republiku a Slovenskú republiku v Brne (info.cz@beckhoff.com), ktorí vám radi pomôžu.

BECKHOFF

Beckhoff Automation s.r.o.

Sochorova 23, 616 00 Brno
Tel.: +420 511 189 255
info.cz@beckhoff.com
www.beckhoff.cz

|atp|journal | Priemyselné PC

SPOLOČNOSŤ FARNELL ROZŠIRUJE SORTIMENT O PRODUKTOVÝ RAD Osram Opto Semiconductors

Spoločnosť Farnell, distribútor produktov a riešení pre vývojárov, rozšírila svoju ponuku polovodičových produktov pridaním portfólia Osram Opto Semiconductor do svojej globálnej ponuky. Produkty, medzi ktoré patria okrem iného LED diódy, infračervené žiariče, fotodiódy a optické senzory, poskytujú skúseným technikom pri hľadaní vysoko výkonných riešení väčší výber možností.

Osram Opto Semiconductors má viac ako 40 rokov skúseností s vývojom špičkových produktov v oblasti technológií osvetlenia, vizualizácie a snímačov. Rad Osram rozširuje ponuku spoločnosti Farnell s cieľom ponúknuť zákazníkom produkty na podporu aplikácií na trhu, ako sú napríklad automobilový priemysel, mobilné riešenia, inteligentné siete, meranie, priemysel, automatizácia budov, riadenie spotreby energií či infraštruktúra sietí.

Medzi kľúčové produkty, ktoré má spoločnosť Farnell aktuálne v ponuke, patria:

- Rodina infračervených LED diód OSOLON Black: teraz so špeciálnymi verziami pre automobily, ktoré obsahujú verziu s vlnovou dĺžkou 850 nm určenú pre exteriérové aplikácie, ako sú nočné videnie, ochrana chodcov, rozpoznávanie priestoru pred vozidlom a detekcia jazdného pruhu. Nová verzia s vlnovou dĺžkou 940 nm je určená pre interiérové automobilové aplikácie, ako je monitorovanie vodičov, detekcia obsadenosti sedadiel a rozpoznávanie gest. Tieto produkty s rôznou vlnovou dĺžkou a rôznymi objektívmi pokrývajú širokú škálu požiadaviek zákazníkov a môžu byť prevádzkované až do 5A v impulznom režime.
- Fotodiódy radu SFH 2200 – nová generácia je oveľa menšia ako jej predchodcovia. Vyznačujú sa novým konceptom balienia, ktorý umožňuje spájkovanie bez poškodenia až jeden rok po prvom kontakte so vzduchom v porovnaní so štandardnými produktmi, ktoré si túto vlastnosť uchovávajú len tri dni. Nový balík spĺňa prísne požiadavky automobilového priemyslu a je schválený na prevádzkovú teplotu 125 °C. Fotodiódy SFH 2200 spĺňajú požiadavky na kvalifikáciu AEC-Q101-C a sú ideálne na použitie v dažďových senzoch.
- Rad nízkonapäťových LED diód TOPLED E1608 kombinuje menší balík s výnimočnou všestrannosťou, pričom spĺňa veľmi širokú škálu požiadaviek zákazníkov. Sú obzvlášť vhodné pre automobilový priemysel pre aplikácie, ako sú displeje, osvetlenie okolia a podsvietenie spínačov a prístrojov.
- Širokopásmové infračervené LED diódy SFH 4776 sú vhodné na použitie v nových aplikačných sektoroch, ktoré sa otvárajú zavedením techník spektroskopie s využitím vlnovej dĺžky blízkej infračervenému svetlu na meranie parametrov, ako sú obsah vody, tuku, cukru a bielkovín v potravinách a vo farmaceutických výrobkoch.
- Platforma SYNIOS® P2720 sa skladá z 15 rôznych LED produktov s rôznou veľkosťou čipov, s rôznymi výkonovými parametrami a farbami, ktoré možno flexibilne konfigurovať v rámci jednej zástavby, aby vyhovovali rôznym aplikáciám. Jednoduchá škálovateľnosť platformy a voľnosť pri návrhu sú kombinované s vysokou tepelnou spoľahlivosťou a vysokým jasom, čo prináša nové príležitosti a cenové výhody pre výrobcov automobilov a vývojárov v oblasti osvetlenia.

„Pridanie radu produktov spoločnosti Osram Opto Semiconductors ďalej zvyšuje šírku ponuky produktov od spoločnosti Farnell,“ povedal Lee Turner, globálny riaditeľ divízie polovodičov a jednoduchých počítačov v spoločnosti Farnell.

Produkty Osram Opto Semiconductor sú teraz k dispozícii od spoločnosti Farnell v EMEA, Newark v Severnej Amerike a element14 v APAC.

www.premierfarnell.com



PRUDKÝ RAST TRHU KOLABORATÍVNYCH ROBOTOV

Globálny trh s kolaboratívnymi robotmi čaká v nasledujúcich rokoch prudký rast. Do roku 2025 sa predpokladá navýšenie investícií takmer o dvadsaťnásobok – zo 710 miliónov na 12,3 miliárd dolárov. Podiel na trhu rastie vďaka požiadavkám firiem na automatizáciu a pre nedostatok zamestnancov na pracovnom trhu. Na tento trend poukazujú údaje z analýzy spoločnosti Markets and Markets.

Kolaboratívny robot (kobot) je univerzálnejším a flexibilnejším riešením ako tradičný priemyselný robot. Novú kategóriu robotiky prvýkrát predstavil v roku 2008 Dán Esben Østergaard, ktorý je spoluzakladateľom spoločnosti Universal Robots. E. Østergaard chcel, aby bola robotická technológia dostupná všetkým spoločnostiam bez ohľadu na ich veľkosť. Na to vyvinul malé, používateľsky prívetivé, flexibilné a ekonomické roboty, s ktorými môže človek bezpečne pracovať v tesnej blízkosti. V súčasnosti sa čoraz viac spoločností po celom svete rozhoduje využiť na automatizáciu svojich výrobných procesov roboty. Medzinárodná federácia robotiky (IFR) vníma kolaboratívne roboty ako jeden z najdôležitejších technologických trendov, ktoré budú v budúcnosti formovať trh.



Prečo je tento tovar taký žiadaný? Pre malé a stredné firmy, pre ktoré znamená obstaranie tradičných priemyselných robotov príliš veľkú investíciu, predstavujú kolaboratívne roboty cenovo dostupnú alternatívu. Zároveň sú tieto zariadenia používateľsky oveľa prívetivejšie a ľahko sa integrujú do súčasných pracovných procesov bez nutnosti nákladných rekonštrukcií výrobných hál. Zásadná je bezpečnosť kolaboratívnych robotov – vďaka nej môžu pracovať v bezprostrednej blízkosti svojich ľudských kolegov a tí sa môžu venovať kreatívnejším úlohám.

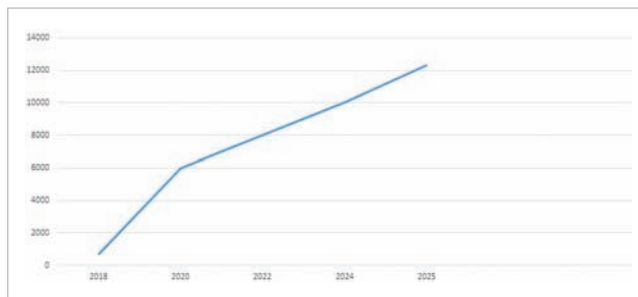
„Kolaboratívne roboty sú čím ďalej, tým viac vyhľadávaným riešením priemyselnej automatizácie, najmä pre nízku obstarávaciu cenu, vďaka ktorej sú dostupné aj pre malé a stredné podniky. Navyše návratnosť investície na obstaranie je veľmi rýchla,“ vysvetľuje rastúci záujem o kolaboratívnu robotiku Pavel Bezucký, obchodný riaditeľ firmy Universal Robots.

Rastúci podiel kobotov na trhu

Nová analýza trhu spoločnosti Markets and Markets Collaborative Robot Market by Payload Capacity, Industry Application, and Geography – Global Forecast to 2025 ukazuje, že tendencia rastu trhu s kolaboratívnymi robotmi neustále stúpa, na čo poukazujú dáta z roku 2018. Zo 710 miliónov dolárov vzrastie do roku 2025 podiel na 12,3 miliárd dolárov. Každý rok sa tak tento segment zväčší o 50,31 %. Analytici tento markantný rast pripisujú hlavne nesporným výhodám kobotov, medzi ktoré patria okrem



iného ich finančná nenáročnosť a rýchla návratnosť pri obstaraní, čo zaujíma najmä malé a stredné podniky. Vysoký záujem o kolaboratívnu robotiku je spôsobený rovnako rastúcou mierou automatizácie vo všetkých priemyselných odvetviach, čo priamo súvisí s konceptom Priemyslu 4.0.



Odhad vývoja investícií do kolaboratívnej robotiky (v miliónoch USD)

„O kolaboratívne roboty je záujem v mnohých priemyselných segmentoch, od potravinárstva cez skladový manažment až po klasickú priemyselnú výrobu. Tieto roboty sú ľahké, ľahko sa premiestňujú v priestore a zamestnanci ich môžu jednoducho naprogramovať na aktuálne požadovanú úlohu,“ uviedol P. Bezucký.

Súčasná situácia na trhu práce je jedným zo základných faktorov motivujúcich podniky hľadať nové možnosti automatizácie výroby a optimalizácie procesov. Podľa údajov Slovenského štatistického úradu bola na Slovensku v prvom štvrtroku 2019 miera nezamestnanosti na úrovni 5,8 %. Napriek tomu trh bojuje s nedostatkom zamestnancov, a to predovšetkým v prevádzkach a sektoroch malých a stredných firiem. Koboty sa tak môžu stať dôležitým prvkom, ktorý tento nedostatok pokryje.



Pozrite si analýzu trhu kolaboratívnych robotov od spoločnosti Markets and Markets.

-mk-

THE FACTORY AUTOMATION COMPANY

FANUC

Automatizácia nebola nikdy jednoduchšia

Rýchla inštalácia, robustné
a spoľahlivé.



**Rýchla návratnosť
investície**



**Profitujte
z bezpečnej
spolupráce
človek-robot**

CR-15iA



**Rýchly
štart výroby**



**Jednoduché
programovanie**



**Kontaktujte nás
+421 37 630 07 59**

YASKAWA „VŠETKO V JEDNOM“: ROBOTIKA A RIADENIE POHYBU

Okrem nových modelov robotov a osvedčených riešení rozhraní venovala spoločnosť YASKAWA na Innovation Forum 2019 pozornosť svojej novej továrni na roboty v Slovinsku.



MotoMINI rozšírilo portfólio robotov YASKAWA MOTOMAN o doteraz svoj najmenší model.

Rok 2019 je oficiálnym začiatkom uvedenia prvého vlastného výrobného závodu na roboty YASKAWA v slovinskom meste Kočevje do prevádzky. Nová výrobná a vývojová kapacita prináša najkratšie možné dodacie termíny a rozšírené možnosti riešení na mieru. Zároveň to pre spoločnosť YASKAWA znamená ešte väčšie priblíženie sa k európskemu trhu a technickým trendom. S investíciami okolo 25 miliónov eur zabezpečuje výrobný závod asi 80 % požiadaviek na roboty v Európe. Zároveň sa podarilo vytvoriť približne 200 nových pracovných miest a ďalšie u európskych dodávateľov.

Okrem nového výrobného závodu na roboty má YASKAWA v súčasnosti ďalšie tri veľké projekty, ktoré posilňujú jej prítomnosť v regiónoch Európy. Vo francúzskom Nantes bolo vybudovaných viac ako 10 000 m² výrobných a kancelárskych priestorov. Vo švédskom Torsås bol postavený nový výrobný závod s kancelárskymi priestormi. Začiatkom roku 2018 sa spoločnosť presťahovala do európskej centrály pre robotiku v Allershausene, kde pribudli výrobné a skladovacie priestory s celkovou rozlohou 4 000 a 1 200 m² kancelárskych priestorov.

MotoMINI rozširuje rad najmenších modelov MOTOMAN

Aj v oblasti nových modelov robotov došlo k viacerým zmenám: nový MotoMINI je najmenším modelom v portfóliu robotov MOTOMAN. S pracovným dosahom 350 mm zvládne užitočné zaťaženie 500 g. Kompaktný šesťosový ľahký vysokorychlostný robot kombinuje rýchlu prevádzku s vysokou presnosťou opakovania 0,02 mm. MotoMINI je ideálny na manipuláciu s malými obrobkami a komponentmi, ako



Pomocou softvéru MotoLogix možno roboty YASKAWA MOTOMAN rýchlo a ľahko programovať a ovládať pomocou PLC.

aj na montážne práce v malých výrobných strojoch. Jeho kompaktná forma umožňuje flexibilitu a priestorovo úspornou implementáciu.

Pri veľmi malej zastavanej ploche dokáže tento robot pohybovať s komponentmi vo všetkých troch smeroch a okolo troch osí. Takáto voľnosť pohybu umožňuje realizovať aj zložitejšie priestorové manipulačné úlohy. Prispieva k zmenšeniu priestoru potrebného na výrobné zariadenia a zároveň zvyšuje produktivitu. Pri 7 kg je hmotnosť manipulatora taká nízka, že robot možno nasadiť flexibilne podľa požiadaviek danej prevádzky alebo typu obrobku, ktorý má byť opracovaný.

Nový výkonný ovládač MOTOMAN YRC1000micro

Riadiaca jednotka je tiež malá a ľahká: MotoMINI je ovládaný prostredníctvom vysoko výkonného riadiaceho systému MOTOMAN YRC1000micro. Ručné programovacie zariadenie – ľahšie o 730 g v porovnaní s tými najmenšími vo svojej kategórii – je navrhnuté jednoduchšie a ergonomickejšie. Dotykový displej umožňuje intuitívne ovládanie a tým aj jednoduchší pohyb po obrazovke a rolovanie pomocou kurzora. Na obrazovke ručného zariadenia možno zobraziť 3D simuláciu pohybu skutočného ramena robota a hranice bezpečnej pracovnej oblasti.

Vďaka otvoreným rozhraniám je nová generácia riadiaceho systému predurčená aj na použitie v prostredí Priemyslu 4.0. Mimoriadne kompaktný riadiaci systém s objemom iba 21,5 l možno namontovať do rozvádzača umiestneného vedľa robota do veľmi malého priestoru. Napriek svojej

kompaktnosti ponúka regulátor nielen riadenie pohybu s tradične vysokou kvalitou YASKAWA: môže voliteľne ovládať dve ďalšie osi, môže byť vybavený všetkými zbernicovými systémami a pracovať aj ako bezpečnostný riadiaci systém. Vďaka integrovanému bezpečnostnému regulátoru – až pre 16 rôznych uchopovačov – je táto riadiaca jednotka certifikovaná aj pre PL d kategórie 3, čo je pre spoločnosť YASKAWA už dobrým zvykom.

Softvérové rozhranie MotoLogix teraz s pripojením EtherCAT

Roboty YASKAWA MOTOMAN v aktuálnom prostredí IEC-61131 možno rýchlo a ľahko naprogramovať a ovládať prostredníctvom PLC s nainštalovaným softvérovým rozhraním MotoLogix. YASKAWA rozšírila spektrum podporovaných platforiem vrátane štandardu EtherCAT. Okrem technológie EtherCAT možno použiť aj integrované riešenie na báze POWERLINK, EtherNet/IP a PROFINET. Vďaka tomu možno roboty programovať a riadiť s riadiacimi systémami Siemens, Beckhoff, B&R, Rockwell Automation a samozrejme YASKAWA.

Vďaka integrácii do PLC sú všetky skutočné výhody riadiacej jednotky robota zachované. Riadiaci systém robota počíta pohybovú kinematiku a zaručuje vysokú kvalitu pohybu. To znamená, že know-how spoločnosti YASKAWA je zaručené tam, kde ide o presné pohybové sekvencie manipulatorov. Konkrétne vo všetkých formách manipulácie, ako je nakladanie, vykladanie, balenie, ukladanie, paletizácia alebo meranie, testovanie a triedenie, môžu tieto roboty spolu s príslušnou riadiacou jednotkou naplno preukázať svoju silnú stránku.

Jednoduchá integrácia ovládania robota do PLC sa vyplatí nielen pri prevádzke zložitých výrobných zariadení. S programom MotoLogix postačujú znalosti PLC na riadenie robotov. Vďaka tomu sa eliminuje hľadanie personálu vyškoleného na prácu s robotom alebo nákladné preškolenie pracovníkov. Roboty YASKAWA tak možno prevádzkovať po celom svete rovnakým spôsobom.

YASKAWA

YASKAWA Czech s.r.o.

Business Park Prague Chrástany
Za trati 206, 252 19 Chrástany
Tel.: +420 257 941 718
info.cz@yaskawa.eu.com
www.yaskawa.eu.com

Výrobcovia snímačov tlaku zlepšili presnosť a technológiu, ktorá je inštalovaná do týchto inteligentných meracích zariadení. Mnohé konvenčné kalibračné prístroje sa stali nedostatočnými alebo jednoducho neschopnými testovať a kalibrovať tieto snímače tlaku s vysokou presnosťou.

Vyžadujú sa teda lepšie kalibračné riešenia. Overenie a dokumentácia kalibrácie a nastavenie inteligentného snímača tlaku HART môže vyžadovať kufor plný prístrojov.

Vykonanie takejto úlohy pomocou kalibrátora s komunikáciou HART, ako je Fluke 754, zjednodušuje úlohu a redukuje počet nástrojov, ktoré potrebujete na vykonanie kalibrácie.

Kým začnete kalibráciu v prevádzke

Nainštalujte tlakový konektor na ručný zdroj tlaku. Keď je konektor nainštalovaný, výmena za tlakový modul s iným rozsahom je len otázkou sekúnd bez použitia ďalších nástrojov.

Dosiahnutie požadovanej presnosti

Aby ste dosiahli takú vysokú presnosť ako dnešné prevodníky tlaku, zvolte rozsah tlakového modulu čo najbližšie rozsahu skúšaného prístroja. Priemyselné štandardy odporúčajú presnosť etalónového tlakového modulu aspoň štyrikrát vyššiu, ako je presnosť skúšaného zariadenia. Kalibrátor Fluke 754 podporuje tlakové moduly série 750P a má zabudovanú komunikáciu HART na podporu nastavenia skúšaných snímačov. Dokáže tiež ukladať výsledky kalibrácie pred nastavením a po ňom a vypočítať, či tento výsledok vyhovuje alebo nevyhovuje zadanej špecifikácii.



Ukážka kalibrácie HART prevodníka tlaku pomocou kalibrátora Fluke 754

Ako vykonať kalibráciu

1. Izolujte snímač tlaku od procesu a odpojte jeho elektrické pripojenie. Ak vykonávate meranie prúdu cez diódu prevodníka, nechajte pripojenie zapojené, avšak toto meranie neposkytuje najlepšiu presnosť merania.
2. Pripojte konektory kalibrátora Fluke 754 k prevodníku tlaku.

3. Pripojte kábel tlakového modulu ku kalibrátoru Fluke 754 a prepojte hadičkou ručnú pumpu a snímač tlaku. Stlačte tlačidlo HART na kalibrátore na zobrazenie konfigurácie prevodníka.
4. Stlačte znova tlačidlo HART a kalibrátor ponúkne správnu kombináciu merania/generovania. Ak si želáte dokumentovať kalibráciu, stlačte voľbu As-Found (kalibrácia pred nastavením), vložte toleranciu merania a nasledujúce parametre. Ak je meraný prúdový signál v rámci tolerancie, kalibrácia je kompletná.
5. Zvoľte nastavenie a nastavte tlak prevodníka v nule, prúdový výstupný signál a vstupný senzor.
6. Po nastavení zvolte As-Left (kalibrácia po nastavení), zaznamenajte výstupné parametre prevodníka tlaku po nastavení a ak je výsledok vyhovujúci, kalibrácia je kompletná.



Ukážka kalibrácie HART prevodníka tlaku pomocou kalibrátora Fluke 729

Automatizácia kalibrácie

Automatizáciu kalibrácie prevodníkov tlaku možno vykonať pomocou kalibrátora, ktorý má zabudovanú elektrickú pumpu. Takýmto kalibrátorom je Fluke 729, ktorý bol navrhnutý na automatizáciu prevádzkových kalibrácií. Zabudovaná pumpa automaticky generuje požadovaný tlak v definovaných bodoch. V každom bode sa odčíta hodnota zo zabudovaného etalónového snímača tlaku a zároveň zo skúšaného prevodníka tlaku. Tieto údaje sa priebežne ukládajú

KALIBRÁCIA HART PREVODNÍKOV TLAKU



Kalibrátor tlaku HPC50 s certifikáciou ATEX II 1G IEx ia IIC T4/T3 Ga

do pamäte kalibrátora. Celý proces prebieha automaticky a pred ukončením kalibrácie vás kalibrátor informuje, či skúšaný prístroj vyhovuje alebo nevyhovuje zadanej triede presnosti. Komunikácia HART robí z kalibrátora Fluke 729 ideálny nástroj na kalibráciu v prevádzke.

Kalibrácia v prostredí s nebezpečenstvom výbuchu

Ak sa vo vašej prevádzke nachádza prostredie s nebezpečenstvom výbuchu, je vhodné použiť kalibrátor s adekvátnou certifikáciou. Iskrovo bezpečné kalibrátory Ametek Crystal HPC50 s certifikáciou ATEX do zóny 0 a rozsahom až do 100 MPa možno použiť na kalibráciu snímačov tlaku s analógovým výstupom. Kalibrátor má tiež možnosť pripojenia externých tlakových a teplotných modulov.

Použitá literatúra

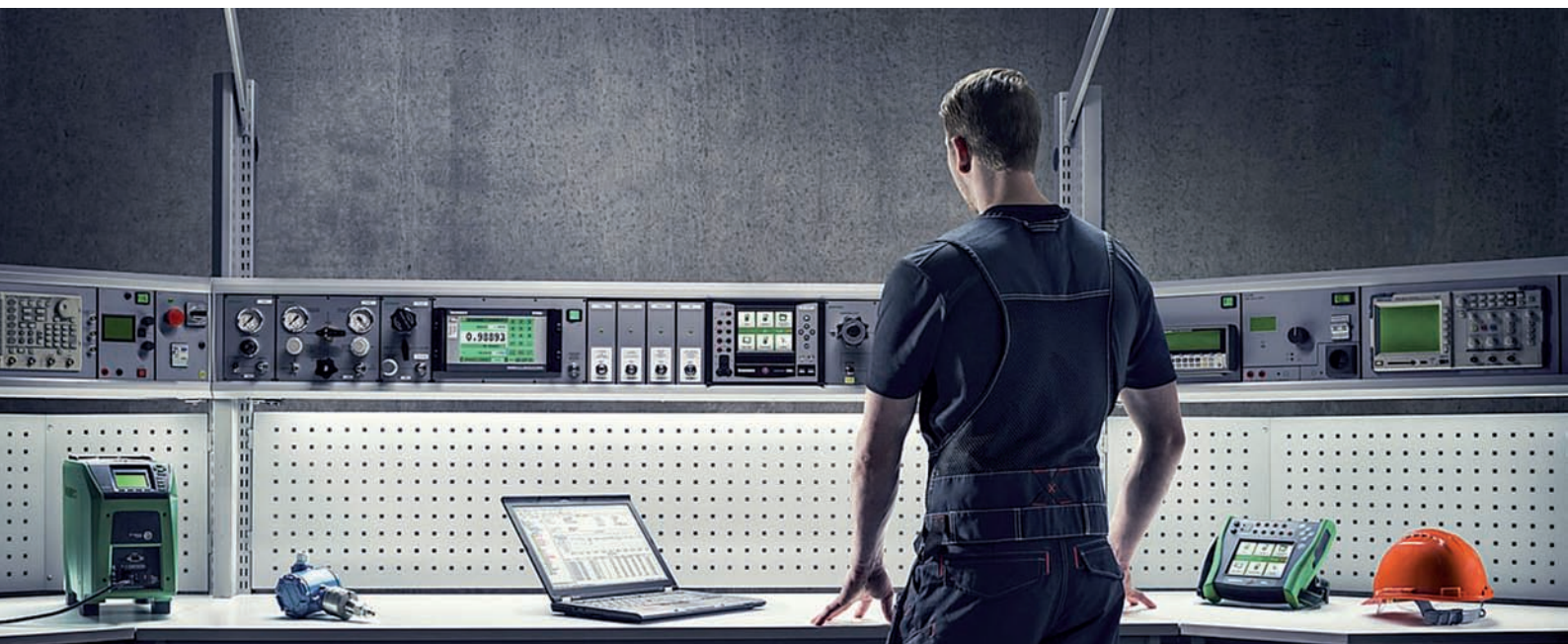
- [1] Fluke Process calibration tools catalog



D-Ex Instruments

Ing. Michal Janoško

D-Ex Instruments, s.r.o.
Pražská 11
811 04 Bratislava
Tel.: 0907 742 744
mjanosko@dex.sk
www.dex.sk



KALIBRAČNÁ NEISTOTA PRE NEMATEMATIKOV

Tento článok hovorí o základoch neistoty pri meraní a kalibrácii. Nie je určený matematikom alebo metrológom, ale tým z vás, ktorí plánujú a realizujú praktické merania a kalibráciu v priemyselných aplikáciách.

V prvom rade si treba uvedomiť neistotu súvisiacu s meraním. Pokiaľ nepoznáte súvisiacu neistotu, nemali by ste merať vôbec. Vo všeobecnosti je dobrou správou, že záujem a povedomie o neistotách pri meraní rastie. O stanovení neistoty merania pri kalibrácii existuje mnoho príručiek, noriem a dostupných zdrojov väčšinou plných matematických vzorcov, takže v tomto článku sa pokúsime udržať minimálnu možnú úroveň matematiky. Toto je praktická príručka, ktorá vám pomôže získať všeobecné znalosti vo veľkom svete neistôt pri meraní a kalibrácii.

merania. Tiež testovala rozťahovanie struny, no to nemalo vplyv na výsledok merania.

Tento zjednodušený príklad ukazuje, že výsledok merania ovplyvňuje mnoho faktorov – použité meracie prístroje, meracie metódy, proces merania a spôsob realizácie samotného merania.

Otázka, ktorú by ste si mali položiť, znie: Ak vykonávate vo vašom závode kalibračné práce, ktorý z týchto troch prípadov vám znie najpravdepodobnejšie u Vás používaný? Aký druh „pravítka“ používate vo vašej prevádzke a aké sú metódy a procesy merania? Ak ste už niečo odmerali bez zistenia súvisiacej neistoty, výsledky za veľa nestoja.

Veľmi krátky terminologický kurz

Pozrime sa na veľmi stručný prehľad základných pojmov súvisiacich s touto témou. Čo je vlastne neistota merania? Jednoducho môžeme povedať, že je to „pochybnosť“ nášho merania a hovorí o tom, aké dobré to naše meranie je. Každé zrealizované meranie má svoje „pochybnosti“ a mali by ste vedieť, aká veľká tá „pochybnosť“ v skutočnosti je, aby ste vedeli rozhodnúť o kvalite merania na daný účel.

Je dobré si uvedomiť, že chyba nie je to isté ako neistota. Ak porovnáme naše zariadenie, ktoré sa chystáme kalibrovať, s etalónom, chyba je rozdiel medzi týmito dvoma zariadeniami. Chyba však nemá žiadny význam, pokiaľ nepoznáme neistotu merania.

Preto je dôležité povedať: Ak nepoznáte neistotu merania, nemerajte radšej vôbec!

Príliš často vidíme príklady, keď človek meria v procese s prípustným limitom $\pm 1,0$ °C a zistí maximálnu chybu 0,5 °C; je šťastný a hovorí, že meranie „prešlo“ a akceptuje výsledky, hoci po analýze procesu kalibrácie zistí, že celková neistota jeho procesu merania je $\pm 2,0$ °C. Čiže spôsob vykonanej kalibrácie nebol pre danú aplikáciu dosť dobrý. No pokiaľ o neistote nevedel alebo sa o ňu nezaujímala, mohol tvrdiť, že to bola dobrá kalibrácia, hoci v skutočnosti zlyhala.

V prvom rade si treba uvedomiť neistotu súvisiacu s meraním. Pokiaľ nepoznáte súvisiacu neistotu, nemali by ste merať vôbec. Vo všeobecnosti je dobrou správou, že záujem a povedomie o neistotách pri meraní rastie.

Klasický príklad merania „kúska špagátu“

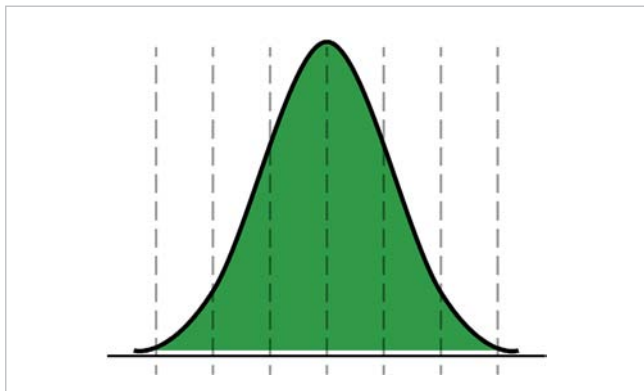
Začnime ilustračným príkladom merania neistoty v praxi. Tri osoby postupne dostanú rovnakú strunu a požiadame ich, aby zmerali jej dĺžku. Žiadne iné inštrukcie nedostanú. Všetci môžu použiť svoje vlastné nástroje a meracie metódy. Je viac ako pravdepodobné, že získame tri rôzne odpovede, napríklad:

- Prvá osoba hovorí, že struna má dĺžku 60 cm. Na meranie použila 10 cm dlhé plastové pravítko, strunu odmerala raz a takto dospela k tomuto záveru.
- Druhá osoba tvrdí, že struna má dĺžku 70 cm. Použila trojmetrový stáčací meter a získaný výsledok niekoľkokrát skontrolovala, aby sa uistila, že má pravdu.
- Tretia osoba hovorí, že dĺžka struny je 67,5 cm s neistotou $\pm 0,5$ cm. Použila presný stáčací meter a strunu niekoľkokrát zmerala. Získala tak priemernú hodnotu a smerodajnú odchýlku

Od jedného merania až po zistenie smerodajnej odchýlky

Ako by ste teda mali začať svoju cestu poznania všetkých súvisiacich neistôt? Prvým jednoduchým, no dobrým postupom je, že pri normálnom meraní či kalibrácii skúste opakovať rovnaké meranie niekoľkokrát. S najväčšou pravdepodobnosťou zistíte malé rozdiely vo výsledkoch merania medzi opakovaniami. Ktoré meranie je správne?

Bez prílišného zachádzania do štatistiky môžeme povedať, že nestačí merať iba raz. Ak opakujete rovnaké meranie niekoľkokrát, môžete nájsť priemernú hodnotu a smerodajnú odchýlku merania. Takto zistíte, ako veľmi sa výsledky medzi opakovaniami líšia, a zároveň sa dozviete aj normálny rozdiel medzi meraniami. Odporúča sa vykonávať merania niekoľkokrát, dokonca až desaťkrát, aby boli štatistiky dostatočne spoľahlivé na výpočet smerodajnej odchýlky.



Obr. 1 Smerodajná odchýlka

Tento typ neistoty získaný výpočtom smerodajnej odchýlky sa nazýva neistota typu A.

Môžete povedať: „Čože? V praxi nemožno opakovať jedno meranie desaťkrát! Našťastie nemusíte vždy robiť desať opakovaní, ale mali by ste stále experimentovať s vaším meracím procesom tak, aby ste niekedy zopakovali to isté meranie. To vám napovie, aká je typická odchýlka celého procesu merania a na základe tejto znalosti ju môžete v budúcnosti použiť ako súčasť neistoty súvisiacej s týmto meraním – a to aj v prípade, že meriate len raz počas bežnej kalibrácie.

Predstavte si, že by ste vykonávali meranie alebo kalibráciu teploty viackrát a zistili by ste, že medzi opakovaniami môže byť rozdiel $\pm 0,2$ °C. Keď urobíte to isté meranie nabudúce (aj keď iba raz), mali by ste počítať s existujúcim možným rozdielom $\pm 0,2$ °C a nechať meranie príliš blízko limitnej hodnoty.

Takže ak budete stále opakuovať kalibráciu podobných druhov prístrojov, treba často vykonávať meranie len raz a použiť typickú experimentálnu smerodajnú odchýlku. Svoju domácu úlohu si, samozrejme, urobiť musíte a merania a výpočty by mali prebiehať tak, aby ste zistili smerodajnú odchýlku daného nástroja a kalibračného procesu. Stručne povedané, stále by ste mali vedieť smerodajnú odchýlku vášho kalibračného procesu – je to jedna časť celkovej neistoty merania.

Váš etalón (kalibrátor) a jeho nadväznosť

Jedným z najväčších zdrojov neistôt je často etalón (referenčný prístroj alebo kalibrátor), ktorý používate pri meraní alebo kalibrácii. Prirodzene na začiatku by ste mali zvoliť na každé meranie vhodný etalón. Dôležité je uvedomiť si, že nestačí použiť špecifikáciu výrobcu týkajúcu sa presnosti etalónu a používať ju dlhé roky ako neistotu etalónu. Namiesto toho musíte svoje etalóny pravidelne kalibrovať v kalibračnom laboratóriu s dostatočnými schopnosťami (dostatočne malá neistota) a zaistiť tak ich metrologickú nadväznosť. Dbajte na celkovú neistotu kalibrácie, ktorú laboratórium zdokumentovalo pre váš etalón. Tiež by ste mali udržiavať stabilitu vašich etalónov pomocou pravidelnej kalibrácie. Po určitom čase získate skutočnú neistotu vášho etalónu a túto informáciu môžete použiť ako neistotu etalónu pri kalibrácii.

Iné zdroje neistoty

V predchádzajúcej časti som navrhol opakovať meranie niekoľkokrát. No čo by sa stalo, keby ste požiadali svojich kolegov, aby zopakovali to isté meranie? Získajú všetci rovnaké výsledky? Často vznikajú medzi rôznymi merajúcimi osobami určité rozdiely. Znamená to teda, že osoba vykonávajúca meranie má tiež vplyv na neistotu? Áno. Platí to hlavne vtedy, ak nie sú inštrukcie na dostatočnej úrovni.

Čo ak vykonáte rovnaký test a tentoraz použijete na meranie rôzne etalóny (kalibrátory)? Opäť s najväčšou pravdepodobnosťou natrafíte na rozdiely. A ak majú etalóny rôznu úroveň presnosti (neistoty), možno dokonca badať relatívne veľké rozdiely. Často je etalón (alebo kalibrátor) používaný na meranie jedným z najväčších zdrojov neistoty!

Rôzne environmentálne podmienky môžu pri určitej kalibrácii pridať ďalšiu neistotu.

Ak potrebujete odčítať výsledky z analógového displeja (deformačný tlakomer, teplomer), máte obmedzenú odčítateľnosť, t. j. môžete ich prečítať iba s určitou presnosťou a navyše nesprávne (nesprávny uhol pohľadu), čo pridáva neistotu. V prípade digitálneho odčítania je rozlíšenie (počet desiatinných miest) vždy obmedzené, čo spôsobuje neistotu (môžete odčítať iba posledné desiatinné číslo).

Rôzne technické aspekty v procese kalibrácie a rôzne ovplyvňujúce veličiny pridávajú ďalšiu neistotu. Napríklad pri kalibrácii teploty je nevyhnutné čakať dostatočne dlho, než sa teplota stabilizuje a treba zabezpečiť správne ponorenie snímača do teplotného bloku; pri kalibrácii prietoku musíte zabezpečiť stabilný prietok; pri kalibrácii tlaku sa musíte vyhnúť únikom a musíte mať stabilný tlak atď. Vo všeobecnosti akékoľvek zmeny alebo výkyvy meranej veličiny spôsobujú ďalšiu neistotu. Netreba zabúdať na ďalšie náhodné premenné, ktoré pridávajú do „polievky ďalšie korenia“. Takisto môžete použiť experimentálnu smerodajnú odchýlku spomenutú vyššie ako jednu zo súčastí neistoty.

Stručne si môžeme zhrnúť tieto dodatočné zdroje neistoty:

- kalibrované meradlo,
- etalón (kalibrátor),
- metóda/postup na realizáciu merania/kalibrácie,
- environmentálne podmienky,
- osoba (osoby) vykonávajúca meranie,
- ďalšie zložky neistoty závislé od meranej veličiny.

Všetky uvedené zložky neistoty sa označujú ako neistota typu B.

Spojenie jednotlivých neistôt => kombinovaná neistota

Neistotu typu A (smerodajná odchýlka) možno vypočítať, ale často treba odhadnúť niektoré z iných neistôt typu B. Po vypočítaní smerodajnej odchýlky a odhadnutí rôznych neistôt typu B je čas na ich spočítanie. Predtým sa musíte uistiť, že všetky neistoty sú v rovnakej veličine/jednotke. Neistoty by mali mať tiež rovnaký faktor pokrytia/úroveň spoľahlivosti.

Ak spájate čiastkové neistoty, ktoré sú od seba nezávislé, nesčítavajte ich dohromady, mohlo by to priniesť príliš pesimistický výsledok (najhorší prípad). Namiesto toho spojte jednotlivé neistoty



ako sumu druhých mocnín pod odmocninou. Znamená to, že každú čiastkovú neistotu umocníte, takto ich sčítate a nakoniec vezmete druhú odmocninu z celkového súčtu.

Hoci sme povedali, že žiadne vzorce v článku nebudú, možno bude ľahšie vyjadriť kombinovanú neistotu relatívne jednoduchým vzorcom.

Celková neistota =

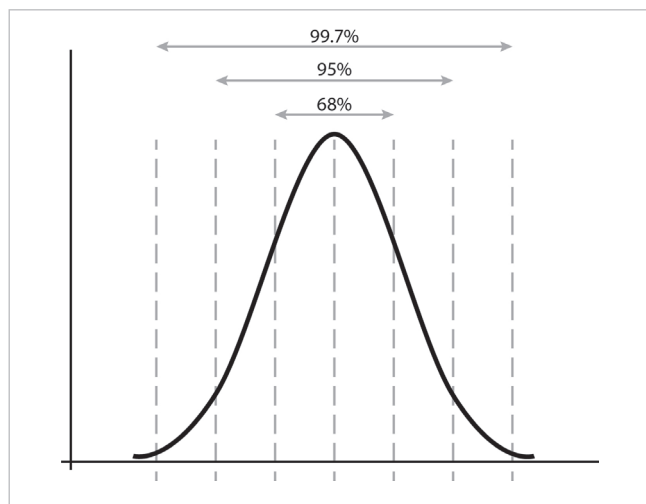
$$\sqrt{u_{(1)}^2 + u_{(2)}^2 + \dots + u_{(n)}^2}$$

kde každé u je jedna nezávislá súčasť neistoty.

Faktor pokrytia/úroveň spoľahlivosti

Po určení kombinovanej neistoty sa zvyčajne ešte vynásobí koeficientom pokrytia (k). Najčastejšie sa kombinovaná neistota vynásobí 2 ($k = 2$ alebo 2 sigma). Toto násobenie je dôležité na dosiahnutie vyššej úrovne spoľahlivosti. Použitie faktora pokrytia 2 zodpovedá úrovni spoľahlivosti 95 %, keďže sa zaoberáme štatistickými údajmi a podľa normálneho (Gaussovoho) rozdelenia je 95 % výsledkov v rozsahu 2 sigma. V praxi teda bude vďaka 2 sigma 95 % výsledkov v danom rozsahu neistoty. Rôzne hodnoty sigma nám dávajú nasledujúce úrovne spoľahlivosti:

- 1 sigma ($k = 1$) = úroveň spoľahlivosti 68 %,
- 2 sigma ($k = 2$) = úroveň spoľahlivosti 95 %,
- 3 sigma ($k = 3$) = úroveň spoľahlivosti 99,7 %.



Obr. 2 Normálne (Gaussovo) rozdelenie

Ak spájate jednotlivé čiastkové neistoty, uistite sa, že všetky sú v rovnakej sigma hodnote ešte pred spojením.

Rozšírená neistota

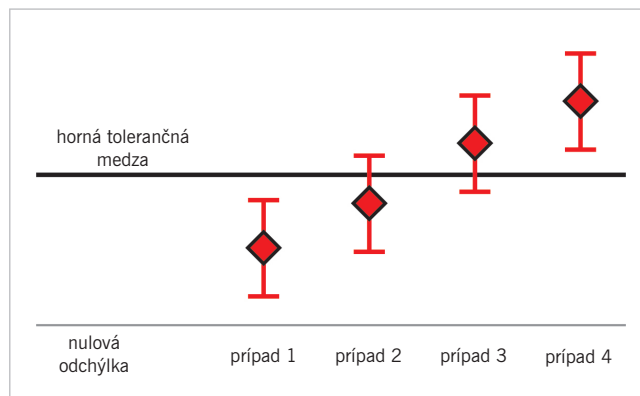
Pred zverejnením kombinovanej neistoty, aby ste sa dostali na požadovanú úroveň spoľahlivosti, musíte vynásobiť výsledok s vybraným koeficientom rozšírenia (faktorom pokrytia). Po násobení získate rozšírenú neistotu, t. j. neistotu zodpovedajúcu určitej úrovni spoľahlivosti.

Ako vyjadriť neistotu vo výsledkoch alebo kalibračnom certifikáte

Vo výsledkoch kalibrácie by ste mali vyjadriť neistotu ako $\pm$ hodnotu, pričom treba uviesť faktor pokrytia/úroveň spoľahlivosti. Napríklad môžete povedať, že teplota je: 20,5 °C s neistotou $\pm 0,1$ °C ($k = 2$).

Vyhlasenie o zhode – vyhovel alebo nevyhovel

Kalibrácia prístroja najčastejšie obsahuje akceptačné kritérium, t. j. hranice, v rámci ktorých sa výsledok považuje za vyhovujúci a mimo ktorého sa považuje za nevyhovujúci. Existujú mnohé interpretácie, či a ako by sa mala zohľadniť neistota pri rozhodovaní o zhode. Zoberme si niekoľko príkladov ako ukážku. Obr. 3



Obr. 3

znázorňuje výsledky merania, čiary pod a nad označujú celkovú neistotu merania.

Uvedené prípady môžeme interpretovať takto:

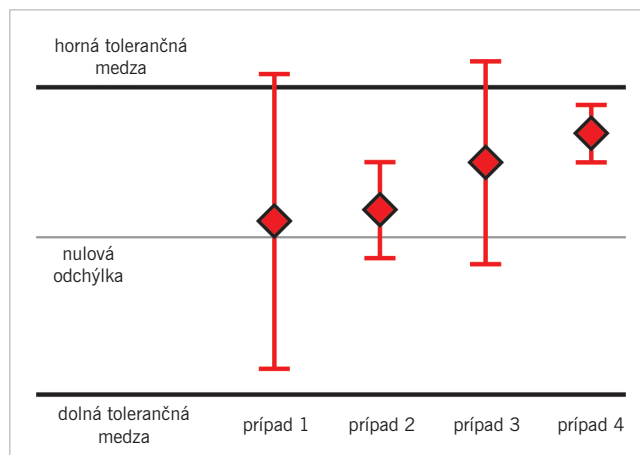
- Prípady 1: Tento prípad je celkom jasne v rámci tolerančných hraníc aj pri uvažovaní s neistotou.
- Prípady 2: Toto je tiež celkom jasný prípad. Výsledok je mimo tolerančných hraníc aj s uvažovaním neistoty. Môžeme konštatovať, že ide o zlý alebo „nevyhovujúci“ výsledok.
- Prípady 3 a prípady 4: Tieto prípady sa dajú posúdiť trochu ťažšie. Síce sa zdá, že výsledok v prípade 2 je v tolerancii a výsledok 3 je mimo – hlavne, ak vás nezaujíma neistota. No ak vezmete do úvahy neistotu, s istotou nemôžeme posúdiť ani jeden prípad.

Postup pri posudzovaní zhody je opísaný podrobne v dokumentoch (napríklad ILAC G8: 03/2009 Pokyny na posudzovanie a vykazovanie zhody so špecifikáciami; EURACHEM/CITAC Guide: Použitie informácií o neistote pri posudzovaní zhody, prvé vydanie z roku 2007). Tieto príručky naznačujú, že výsledok merania je vyhovujúci len vtedy, keď je chyba zväčšená o neistotu menšia ako hranica akceptácie. Tiež navrhujú považovať výsledok za nevyhovujúci len vtedy, keď je chyba s odčítanou neistotou väčšia ako hranica akceptácie. Keď je výsledok bližšie k akceptačnej hranici viac ako o polovicu neistoty, odporúča sa nazvať situáciu „nedefinovanou“, t. j. nesmieme uviesť ani vyhovel, ani nevyhovel.

Mnohí interpretujú neistotu a rozhodnutie vyhovel/nevyhovel rôznymi spôsobmi. V praxi sa neistota najčastejšie neberie do úvahy pri rozhodovaní o zhode so stanovenou špecifikáciou, ale je veľmi dôležité byť si vedomý neistoty merania pri kalibrácii pri rozhodovaní.

Príklady neistoty

Na obr. 4 je niekoľko prípadov rôznych neistôt v praxi. Prípady 1 a 2 majú rovnaký výsledok merania, čiže bez neistoty by sme považovali obe merania za rovnaké. Keď sa však vezme do úvahy neistota, môžeme vidieť, že prípad 1 je naozaj hrozny, pretože neistota je príliš veľká na to, aby sa mohla použiť na meranie s danými tolerančnými medzami. Pohľad na prípady 3 a 4 ukazuje, že prípad 3 je lepší,



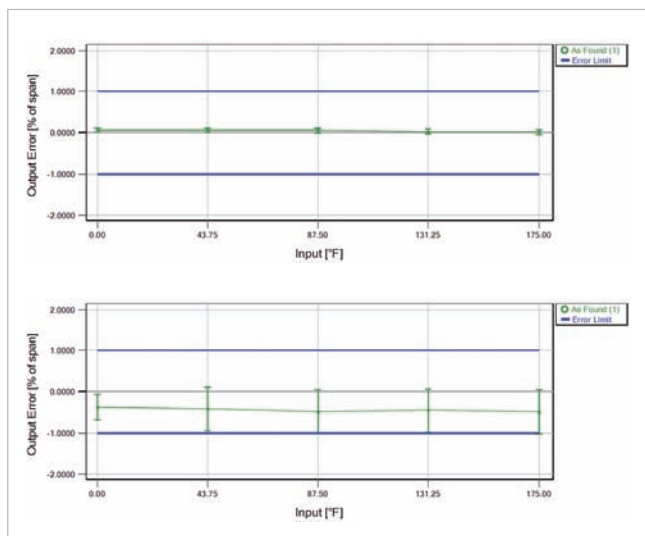
Obr. 4

no s neistotou je viditeľné, že to nie je dostatočné na rozhodnutie vyhovet, no prípad 4 je dostatočný.

Zase chcem poukázať na to, že je dôležité poznať neistotu predtým, než sa rozhodneme o výsledkoch merania. Bez výpočtu neistoty vyzerajú prípady 1 a 2 rovnako, hoci s uvažovaním neistoty sú veľmi rozdielne.

Príklad zo skutočného života

Nižšie uvedený príklad zo skutočného života používa rovnaký odporový snímač teploty kalibrovaný pomocou dvoch rôznych kalibrátorov. Tento obrázok bol vytvorený pomocou kalibračného softvéru Beamex CMX. V prvom prípade je ľahké vidieť, že výsledky sú veľmi dobré, vertikálna čiara znázorňujúca neistotu je veľmi krátka, čo naznačuje veľmi malú neistotu. V druhom prípade je vidieť, že výsledok je o niečo horší, ale neistota tohto kalibrátora je oveľa horšia. Netreba dodávať, že v prvom prípade bol použitý kalibrátor Beamex. V každom prípade, keď vidíte neistotu zobrazenú graficky, je veľmi ľahké uvedomiť si jej význam.



Obr. 5

TUR verus výpočty neistoty

V rôznych publikáciách sa často uvádza TUR (pomer neistôt pri kalibrácii). V skratke to znamená, že ak chcete kalibrovať 1 % prístroj a chcete mať pomer 4 : 1, vaše testovacie zariadenie by malo byť štyrikrát presnejšie, t. j. malo by mať presnosť 0,25 %

alebo lepšiu. Niektoré publikácie uvádzajú, že s veľkým pomerom TUR sa netreba starať o výpočet/odhad neistoty. Najbežnejšie odporúčaný pomer TUR je 4 : 1. Niektoré návody a publikácie majú vlastné odporúčania pre TUR. Najčastejšie sa tento pomer používa ako vo vyššie uvedenom prípade, t. j. len na porovnanie špecifikácie presnosti DUT (skúšaného zariadenia) a výrobcom uvádzanej špecifikácie etalónu. No v tomto prípade uvažujete iba špecifikáciu etalónu (testovacieho zariadenia, kalibrátora) a neberiete do úvahy všetky ostatné neistoty. Toto riešenie môže byť „dostatočne dobré“ pre niektoré kalibrácie, ale systém neberie do úvahy niektoré z najväčších zdrojov neistôt. Preto sa odporúča vyhodnotiť neistotu celého kalibračného procesu.

Často sa nás pýtajú: „Koľkokrát presnejší by mal byť kalibrátor v porovnaní s prístrojom, ktorý sa má kalibrovať?“ Niekoľko návrhov sme síce uviedli, no len jedna správna odpoveď na túto otázku neexistuje. Namiesto toho by ste si mali byť vedomí celkovej neistoty vašich kalibrácií. A to by malo, samozrejme, odrážať vaše potreby!

Zaujímavé odkazy na súvisiace dokumenty: EA-4/02 M: 2013, ILAC-G8/2009, JCGM 100: 2008, JCGM 106: 2012.

Zhrnutie

Dúfame, že tento článok prispel k praktickému pochopeniu problematiky neistoty. Krátko zhrnieme kľúčové informácie z hlavných tém:

- Nezabudnite rozlíšiť „chybu“ a „neistotu“.
- Experimentujte s počtom opakovaní merania, aby ste získali viac informácií o typickej smerodajnej odchýlke.
- Používajte vhodné etalóny (kalibrátory) a uistite sa o ich metrologickej nadväznosti a o tom, že neistota kalibrácie je známa a vhodná pre vaše aplikácie.
- Zvážte, či má prostredie významný vplyv na neistotu merania.
- Uvedomte si odčitateľnosť a rozlíšenie displeja na všetkých zobrazovacích zariadeniach.
- Preštudujte si špecifické faktory o veličinách, ktoré sú predmetom vašich kalibrácií.
- Oboznámte sa s „druhou odmocninou súčtu druhých mocnín“ a spojte nezávislé neistoty.
- Uvedomte si faktor pokrytia/úroveň spoľahlivosti použitý pri rozšírenej neistote.
- Namiesto alebo ako súčasť pomeru TUR sa snažte byť viac informovaný o všetkých súvisiacich neistotách.
- Dbajte na celkovú neistotu kalibračného procesu ešte pred rozhodnutím o zhode.

Zdroj: <https://blog.beamex.com/>

www.beamex.com

Beamex MC6-Ex

Nový iskrovo bezpečný prevádzkový kalibrátor a komunikátor!



www.beamex.com
info@beamex.com

beamex
A BETTER WAY TO CALIBRATE

- ATEX a IECEx certifikácia pre všetky zóny v prostredí s nebezpečenstvom výbuchu.
- Veľmi presný kalibrátor dodávaný s kalibračným listom z akreditovaného kalibračného laboratória.
- Umožňuje plne elektronický a automatizovaný postup kalibrácie.
- Vstavaný prevádzkový komunikátor pre protokoly HART, FOUNDATION Fieldbus a Profibus.
- Multifunkčný prevádzkový kalibrátor tlaku, teploty a elektrických veličín.

Kalibrátory, s.r.o.

info@kalibratory.sk
www.kalibratory.sk

OPEN SOURCE IIoT Gateway RevPi Connect S VÄČŠOU PAMÄŤOU



Krátko po uvedení nového radu Raspberry Pi Compute Module 3+ spoločnosť Raspberry Pi Foundation nemecká firma KUNBUS vybavila aj RevPi Connect+ týmito modulmi. V porovnaní s predchádzajúcim modelom s 4 GB pamäťou eMMC majú teraz nové zariadenia 8, 16 alebo 32 GB pamäť eMMC.

Open source IIoT Gateway RevPi Connect+ ponúka používateľovi maximálnu slobodu dizajnu pri implementácii jeho IIoT projektov, a to vďaka koncepcii otvorenej platformy (vrátane plných práv root). RevPi Connect+ sa montuje na DIN lištu a je vybavený dvomi ethernetovými portmi RJ45, dvomi USB portmi a rozhraniami RS485, Micro-HDMI a Micro-USB. Jeho dve ethernetové rozhrania podporujú súčasnú integráciu do automatizačných a IT sietí. To napríklad znamená, že dáta zo zariadenia alebo stroja sa dajú bezpečne preniesť priamo do cloudu alebo nadradeného systému ERP. Na to sú používateľovi k dispozícii známe protokoly ako MQTT a OPC UA. Jednotlivé aplikácie možno naprogramovať napr. pomocou Node-RED, Python alebo priamo v C.

K IIoT Gateway RevPi Connect založenej na Raspberry Pi pribudli ďalšie modely, takže je teraz k dispozícii vo verzii s až 32 GB pamäťou eMMC pod názvom RevPi Connect+. Zariadenie je navrhnuté ako výkonná IIoT brána a obsahuje dve ethernetové rozhrania, hardvérový watchdog a možnosť pripojenia vhodných I/O, gateway a rádiových modulov.

Vďaka modulárnej konštrukcii možno základný modul doplniť vhodnými rozširujúcimi modulmi, ako sú IO moduly, brány priemyselných zberníc PROFIBUS, PROFINET, EtherCat alebo rádiové moduly pre M-Bus. Tieto rozširujúce moduly sa pripájajú k základnej jednotke cez konektor plug-and-play na hornej strane a ľahko sa konfiguruje cez grafické používateľské rozhranie.

Ako operačný systém sa používa prispôbený Raspbian s real-time Linux. Okrem toho RevPi Connect+ už disponuje funkciami Master a Slave široko používaných protokolov Modbus RTU a Modbus TCP. Integráciu do iných zberníc alebo priemyselných ethernetových sietí možno realizovať pomocou vyššie uvedených rozširujúcich modulov. Voliteľne dostupný riadiaci a HMI softvér tiež umožňuje rozšírenie brány IIoT na malý priemyselný controller.

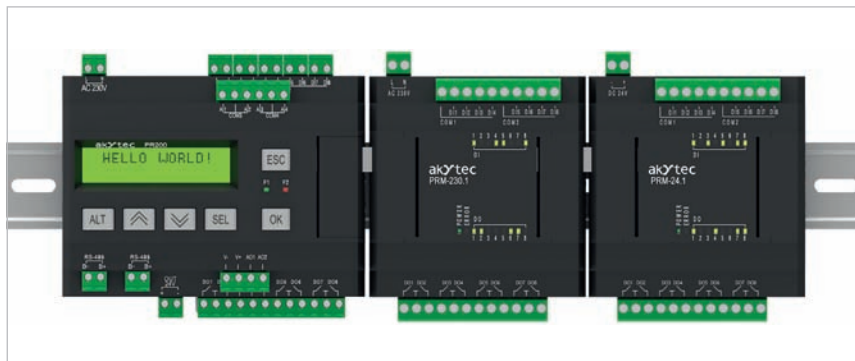
**CONTROL
SYSTEM**

ControlSystem, s.r.o.

Štúrova 4
977 01 Brezno
Tel.: +421 48 61 15 900
info@controlsystem.sk
www.controlsystem.sk

MINI PLC S VYSOKÝM POTENCIÁLOM

Od domácej automatizácie až po priemyselné použitie: programovateľným relé PR200 ponúka firma akYtec GmbH mini PLC na univerzálne použitie. Spoločnosť so sídlom v Hannoveri uviedla na trh rozširujúci modul, ktorým ešte zvýšila flexibilitu tohto mini PLC. Rozširujúci modul PRM je doplnok programovateľného relé PR200. Má rovnaký výkon ako základná jednotka a ponúka osem ďalších digitálnych vstupov a osem digitálnych výstupov; možné sú až dve rozšírenia, čo zvyšuje potenciál PR200 pri riadení procesov. Modul PRM je k dispozícii vo verziách s napájaním 24 V DC alebo 230 V AC. Prístroj má kompaktné rozmery a možno ho ľahko inštalovať na 35 mm lištu DIN. Vďaka kompaktným rozmerom možno moduly PRM inštalovať nielen v rozvádzačoch, ale aj v ovládacích skrinkách. K programovateľnému relé PR200 je modul PRM pripojený cez internú zbernicu.



Malé a výkonné programovateľné relé PR200 vyvinula spoločnosť akYtec GmbH v roku 2014 a odvtedy sa úspešne etablovalo na trhu ako cenovo efektívna alternatíva ku klasickým PLC. Toto zariadenie je vhodné najmä na správu automatizačných systémov v bytovom priemysle a komunálnych službách, v poľnohospodárstve

a ďalších odvetviach priemyslu. V roku 2019 spoločnosť akYtec predstaví ďalšie rozširujúce moduly, ktoré budú obsahovať analógové vstupy a výstupy, na lepšie prispôbenie programovateľného relé PR200 potrebám zákazníkov a ich projektov.

www.akytec.com

„ČO NAJNESKÔR, AKO SA DÁ, AVŠAK HNEĎ, AKO JE POTREBNÉ.“

Opatrenia na prediktívnu údržbu sa pri komponentoch Murrelektronik vrátia často už pri prvom výpadku, ktorému bolo možné zabrániť.

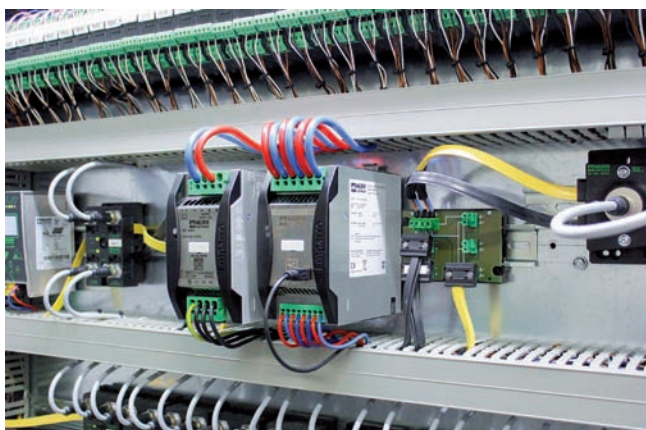
Z hľadiska hospodárnosti strojov a zariadení je smerodajným faktorom možnosť čo najlepšie využiť výkonnosť komponentov vo forme maximálnej doby prevádzky. Murrelektronik kladie preto pri komponentoch elektrického napájania veľký dôraz na to, aby sa vymieňali v optimálnom čase, „čo najneskôr, ako sa dá, avšak hneď, ako je potrebné“.

Ten, kto využíva komponent až do „trpkého“ konca, riskuje neplánované prestoje stroja. Môže si však byť istý, že konštrukčný diel využije maximálne. Nebude mať však radosť z nákladov, ktoré budú potrebné časovo alebo peňažne na opätovné nabehnutie výroby. Skôr defenzívny postup spočíva v tom, že sa komponenty zariadenia vymenia včas, teda v okamihu, do ktorého bežali s absolútnou istotou. To sa dá dobre zorganizovať, má to však svoju nevýhodu, a to, že sa plytvá zdrojmi.

Koncept prediktívnej údržby je zameraný na nájdenie strednej cesty medzi týmito dvomi extrémnymi variantmi. Snahou tohto konceptu je plne využiť životnosť, zároveň však nespôsobiť žiadne neplánované prestoje stroja – a je tak teda najekonomickejší spôsobom využívania jednotlivých komponentov.

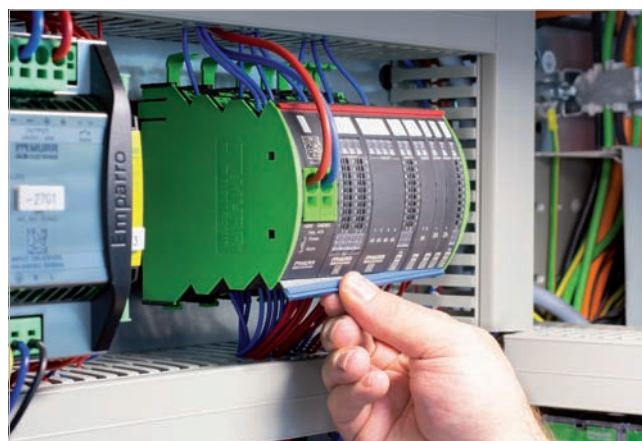
Príkladom z praxe je spínací zdroj Emparro67 Hybrid na použitie v priemyselnom poli (stupeň krytia IP67). Prístroj poskytuje najširšiu škálu diagnostických údajov, ktoré možno bez problémov načítať cez rozhranie IO-Link. Tento prístroj monitoruje prúd, napätie, preťaženie, teplotu, skraty a počet štartov. Na základe týchto údajov je schopný prognózovať zostávajúcu životnosť.

So spínaním zdrojom napájania Emparro 3 ~ 40 A sú kontinuálne monitorované aj údaje ako teplota, počet štartov, vyťaženie a životnosť komponentov. Ak dôjde k prekročeniu niektorej z hraničných hodnôt, prístroj vás upozorní vyslaním signálu. Takto môžete naplávať výmenu v nasledujúcom servisnom intervale.



Emparro ACCUcontrol

Ďalším zaujímavým riešením je USV Modul Emparro ACCUcontrol, ktorý zaručuje neprerušované napájanie prúdom (a teda sám osebe slúži aj na preventívnu údržbu). Integruje sa do mimoriadne citlivých inštalácií strojov a zariadení a v prípade výpadku elektrickej energie udržiava stroje a procesy v chode. Modul monitoruje prevádzku a zvyšnú životnosť pripojených olovených gélových batérií a koordinuje štruktúrované dobíjanie, keď nabíjacia kapacita klesne



Mico Pro

pod určitú hodnotu. Tento proces nabíjania je riadený teplotou s cieľom maximalizovať životnosť batérie. To však stále ešte nie je všetko: informácie sa dajú načítať cez signálny kontakt alebo cez rozhranie USB.

Pokým v doteraz uvedených komponentoch slúžila funkcia preventívnej diagnostiky predovšetkým na vlastnú kontrolu, v prípade inteligentného systému na monitorovanie prúdu Mico Pro je pohľad orientovaný na spotrebiče v inštalácii strojov a zariadení. Mico Pro monitoruje jednotlivé kanály a svietiacou LED diódou (a signálom na výstupe) indikuje, keď sa spotrebúva viac ako 90 % záťaže určenej pre daný kanál. Tak môžete zasiahnuť do procesov predtým, ako by došlo k odstaveniu stroja aktivovaním poistky. Klasickými oblasťami použitia sú „plazivé procesy“, napríklad v dôsledku zvýšenia spotreby elektrickej energie motorov alebo ventilov počas prevádzky.

Murrelektronik kladie pri svojich produktoch veľký dôraz na možnosť prediktívnej údržby, pretože tá podporuje trend smerujúci k stopercentnej bezpečnosti procesov. Klesá počet výpadkov, resp. výpadky sú rýchlo odstránené. V mnohých prípadoch sa finančné náklady investované do opatrení prediktívnej údržby vrátia už pri prvom prestoji, ktorému bolo možné zabrániť. Spoločnosti, ktoré si včas uvedomia dôležitosť tohto prístupu, zvyšujú svoju konkurencieschopnosť, respektíve ju postupujú svojim konečným zákazníkom. Najmä spoločnosti s procesmi, pri ktorých sú prerušenia prevádzky spojené s vysokými nákladmi a v najhoršom prípade dokonca s nebezpečenstvom, sú veľmi otvorené takýmto inováciám. Trend naznačujúci, že výrobcovia strojových zariadení nepredávajú už len stroje a zariadenia, ale formou určitých modelov financovania aj ich dostupnosť, bude prehĺbovať ich prístupnosť voči tejto téme.



Murrelektronik Slovakia s.r.o.

Prievozská 4/B, 821 08 Bratislava
Tel.: +421 2 3211 1127
info@murrelektronik.sk
www.murrelektronik.sk

SPRÁVNÝ PRÍSTUP K VÝBERU A NÁVRHU NAPÁJANIA

Napájací zdroj je kľúčovým prvkom v akomkoľvek návrhu elektroniky a často sa pri ňom zvažuje rozhodnutie o vlastnej výrobe verzus nákupe. Najefektívnejší prístup z hľadiska návrhu závisí od viacerých kritérií a neexistuje univerzálny prístup, ktorý by vyhovoval každej aplikácii.

Existujú tri hlavné možnosti výberu napájacieho zdroja, pričom zložitejšie systémy by sa mohli spoliehať na kombináciu všetkých troch. Prvá možnosť, ktorá bude najznámejšia pre skúsených technikov navrhujúcich dosky plošných spojov, je vlastný napájací obvod, aj keď to často zahŕňa kombináciu bežne dostupných regulátorov výkonu spolu s diskretnými výkonovými tranzistormi a pasívnymi prvkami na filtrovanie a chladenie. Druhým je modul, ktorý spája komponenty nachádzajúce sa v zákazníckom návrhu do jedného balíka, s vonkajšími kolíkmi na uzemnenie, a vstupné a výstupné pripojenie napätia. Takéto moduly sú často úplne zapuzdrené s cieľom ochrany životného prostredia a jednoduchého spájania. Napokon je k dispozícii aj externý zdroj napájania (PSU), ktorý sa môže dodávať vo forme externej jednotky. V prípade, že PSU musí byť integrovaný do systémového rozvádzača, môže byť zakúpený ako produkt s prispôbitelným krytom alebo ako plne uzavretá verzia. Plne uzavretá verzia sa často vyberá pri systémoch, kde sa vyžaduje prístup používateľov, pretože poskytuje najvyššiu úroveň bezpečnosti.

Rozhodnutie, či použiť vlastný návrh, nakonfigurované moduly alebo úplne bežne dostupné zdroje napájania, sa často môže stať záležitosťou tradície. Odpoveď „takto sme to vždy robili“ nemusí však byť nevyhnutne nesprávna, môže to byť záver získaný na základe skúseností. Pri nových projektoch je však namieste prehodnotiť takýto prístup, nakoľko okolnosti a technológie môžu hovoriť v prospech odlišného prístupu.



Legislatíva na celom svete sa neustále vyvíja a zákonodarcovia postupne sprísňujú zákony, ktoré sa týkajú bezpečnosti dodávok a spotreby energie. Napríklad tradičné prístupy založené na pravidlách na získanie bezpečnostnej certifikácie pre zdravotnícke napájacie zdroje sa nahradili hodnotením založenom na riziku, ktoré musí byť podložené dôkazmi. Podobne je to aj s vyhotovením obvodov dodávaných pred piatimi rokmi a vhodných ako zdroje napájania pre spotrebnú elektroniku. Tie teraz nesplňajú nariadenia týkajúce sa spotreby energie v pohotovostnom režime. Legislatíva teraz vyžaduje sofistikovanejšie riadenie a techniky týkajúce sa usmerňovačov, ktoré niektorí vývojári ešte nemusia poznať, aj keď majú dlhoročné skúsenosti v architektúrach na úrovni vývoja dosiek plošných spojov.

Ak nový produkt potrebuje podstatné zmeny v napájacom zdroji, je to pre vývojárov zdrojov príležitosť prejsť na implementáciu založenú

na konfigurovateľných moduloch alebo hotovom PSU. Výrobcovia externých alebo plne balených PSU zvyčajne poskytnú certifikáciu podľa príslušných noriem. Moduly sú vo všeobecnosti navrhnuté tak, aby vyhovovali normám, ale finálne zariadenia, do ktorých idú, budú potrebovať samostatnú certifikáciu.

K podobným úvahám môže viesť aj otázka času uvedenia na trh. Bežne dostupné PSU bude všeobecne znamenať najrýchlejší čas dodávky na trh, ak sa, samozrejme, nájde vhodný zdroj spĺňajúci podmienky danej aplikácie. Aj prispôbenie PSU od dodávateľa tretej strany pridá nejaký čas k celkovému vývoju zariadenia, jeho vyladeniu a výrobe, čo predĺži čas potrebný na uvedenie na trh. Tam, kde je dôležité prispôbenie, poskytujú moduly podstatne väčšiu flexibilitu, ale zároveň budú znamenať predĺženie vývoja a času potrebného na vzájomné prepojenie s ostatnými prvkami, a to najmä tam, kde sa vyžaduje certifikácia. Pre väčšinu projektových tímov budú obe možnosti rýchlejšie ako úplne prispôbené obvody.



Tam, kde ide o veľkosť, môže kompletne navrhnutý obvod ľahko ponúknuť najlepšiu možnosť. Projektant, ktorý pozná požiadavky systému, môže vytvoriť PSU v súlade s ostatnými doskami plošných spojov. Nemusí to byť najmenší možný návrh z hľadiska wattov na centimeter kubický, ale môže to zodpovedať zvyšku systému spôsobom, ktorý minimalizuje objem bez ohrozenia prúdenia vzduchu na chladenie. Moduly sú často navrhnuté s malými rozmermi a nízkymi nákladmi, pričom často využívajú nové techniky balenia na minimalizovanie svojej veľkosti. To môže byť skvelou výhodou v prípade, keď požiadavky cieľového systému zodpovedajú charakteristikám dostupných modulov.

Môžu nastať situácie, keď sú moduly samostatne vysoko kompaktné, ale ich kombinácia potrebná pre cieľovú aplikáciu vedie k nevyužitým miestam a kapacite; tým sa zvýši celková veľkosť a cena riešenia. Situácia s modulmi sa však neustále mení, pretože existuje mnoho modulov, ktoré sú teraz ľahko dostupné prostredníctvom distribútorov, ako je Farnell, čo uľahčuje výber ich kombinácie vyhovujúcej cieľovej aplikácii. Ak má finálny návrh špecifické požiadavky napriek rastúcemu počtu dostupných modulov, tím môže urobiť kompromis na veľkých alebo zmiešaných moduloch s vlastným dizajnom pre špeciálne lišty.

Podobne ako výrobcovia modulov, aj poskytovatelia bežne dostupných PSU môžu využiť výhody úspor z vyššej úrovne výroby a optimalizovaných výrobných technológií s cieľom vytvoriť vysoko kompaktné produkty. V dôsledku toho často ponúkajú návrhy, ktoré poskytujú vysokú hustotu výkonu vyjadrenú vo wattoch na centimeter kubický. Bežne dostupné návrhy však budú často trochu predimenzované, aby bolo možné vybrať pre cieľovú aplikáciu vhodný katalógový produkt. Výsledkom môže byť väčší zdroj, ako sa pre danú aplikáciu požaduje.

Flexibilita návrhu môže byť dôležitým kritériom pre tímy pracujúce so skupinami konkrétnych výrobkov. Ide najmä o situácie, keď prístupy založené na moduloch majú často najväčší zmysel, pretože je relatívne ľahké vymeniť moduly s minimálnym prepracovaním okolitých obvodov. Bežne dostupné PSU sú často k dispozícii vo väčších či menších variantoch a nemusia sa zmestiť do pôvodného formátu. V prípade použitia vlastného obvodu si bude musieť tím nájsť čas na návrh každého variantu, čo môže spôsobiť oneskorenie celého projektu.

Z hľadiska nákladov často dochádza k jasnemu kompromisu medzi vývojom a jednotkovými nákladmi. Jednotkové náklady na štandardne dostupné PSU budú vo všeobecnosti vyššie ako pri modulovom alebo vlastnom dizajne. No hotová jednotka má tú výhodu, že nemá žiadne náklady na vývoj, čo môže byť veľmi dôležité pre projekty s malým objemom. Tam, kde sú dôležité jednotkové ceny, možnosť vlastného návrhu pravdepodobne ponúkne najväčšiu výhodu, hoci vzniknú najväčšie náklady na vývoj.

Hoci vývoj vlastných obvodov zaberie najviac času, vyvinuli výrobcovia rad pomocných nástrojov, ktoré značne zjednodušujú výber a návrh vhodných napájacích zdrojov PCB. Príkladom je EE-Sim DC-DC Design Tool vyvinutý firmou Maxim Integrated. Technik dokáže prostredníctvom intuitívnych formulárov zadať požiadavky špecifické pre danú aplikáciu a získať schému elektrického obvodu, výsledky simulácie a zoznam materiálov ako podporu implementácie.



Minimálna veľkosť, maximálny výkon – zdroje firmy Maxim Integrated

Za zmienku stojí aj to, že čoraz častejšie dochádza k stieraniu hraníc medzi rôznymi typmi riešení napájania. Dodávatelia, ako napríklad TDK-Lambda, používajú modulárne techniky vývoja, aby ponúkli pohodlie bežne dostupných PSU s flexibilitou a výkonom precízne nastavených modulov. Na druhej strane dodávatelia komponentov využívajú integráciu na úrovni balíkov, aby ponúkli vysoko komplexné architektúry napájania, ktoré boli predtým súčasťou kompletne zabalených meničov DC/DC.

Výsledkom je široká škála možností, ktoré môžu vývojárske tímy zvážiť pri výbere ideálnej stratégie napájacích zdrojov pre svoj projekt. Každý projekt sa musí posudzovať zvlášť s využitím kritérií opísaných vyššie. Podrobná analýza požiadaviek odhalí, ktoré riešenie, od štandardne dostupných modulov až po kompletne zákaznické riešenia, najlepšie vyhovuje potrebám aplikácie.

Cliff Ortmeyer

globálny vedúci technického marketingu
Farnell
www.premierfarnell.com

SPOLOČNOSŤ FARNELL ROZŠIRUJE SORTIMENT PRODUKTOV ARDUINO O NOVÉ MODULY MKR

Spoločnosť Farnell, distribútor produktov a riešení pre vývojárov, rozšírila svoju ponuku zabudovaných produktov tak, aby zahŕňala štyri výkonné a kompaktné moduly Arduino MKR Shields s cieľom rozšíriť možnosti a aplikácie dosiek Arduino.



Rozšírená produktová línia spoločnosti Farnell Arduino poskytuje technikom a vývojárom prototypov nový rad príslušenstva, ktorý možno bez problémov integrovať do aplikácií IoT, čím sa zefektívni proces tvorby od prototypu k výrobe. Príslušenstvo Arduino s voľne dostupnou zdrojovou technológiou, s integrovaným pripojením a extrémne nízkou spotrebou energie je vhodné pre širokú škálu IoT aplikácií na koncových zariadeniach napájaných batériou. Všetky tri moduly MKR Shields kombinujú štandardizovaný modulárny rozmerový a výkonový faktor s výkonom 32-bitového mikrokontroléra Arm a možnosťou voľby integrovanej komunikácie prostredníctvom Wi-Fi, GSM, NB-IoT, SigFox alebo LoRa.

Nové produkty, ktoré sú teraz k dispozícii na webovej stránke spoločnosti Farnell, zahŕňajú:

- **Arduino MKR Motor Carrier:** ideálny doplnok pre dosky Arduino MKR, pretože umožňuje používateľom rýchlo vytvárať prototypy a projekty. S MKR Motor Carrier môžu používatelia pripojiť niekoľko motorov a senzorov k ich mechatronickým projektom a riadiť servomotory, jednosmerné či krokové motory. Carrier možno použiť aj na pripojenie ďalších akčných členov a snímačov cez sériu trojkolíkových konektorov.
- **Arduino MKR ENV Shield** vďaka svojmu kompaktnému dizajnu 61 mm x 25 mm, hmotnosti 32 g a vstupnému napätiu 3,3 V umožňuje doskám MKR ľahko zhromažďovať a ukladať údaje o životnom prostredí zozbierané širokým spektrom snímačov. Tie môžu monitorovať atmosférický tlak, teplotu, vlhkosť a intenzitu svetla (LUX) a ultrafialového žiarenia (UVA a UVB). Aby sa zabezpečila plynulá integrácia a zber údajov, je ENV Shield vybavený čítačkou microSD kariet a knižnicou prípravou na použitie a naprogramovanou na čítanie hodnôt z rôznych senzorov.
- **Arduino MKR RGB Shield** – používatelia môžu teraz písať správy a pridávať grafiku, aby zobrazovali hodnoty z dosky MKR. Modul RGB Shield je ovládaný z cloudu Arduino IoT a obsahuje 84 husto osadených a jasných LED diód s plnou farebnou škálou RGB.
- **Arduino MKR Therm Shield:** so vstupným napätím 3,3 V a schopnosťou pracovať pri teplote od 200 do 700 °C umožňuje tento modul doskám MKR vysoko presné meranie teploty v rozšírenom spektre z termočlánkov typu K a digitálnych jednovodičových snímačov DS18Bxx. Dva konektory na module umožňujú použitie termočlánku typu K so zástrčkou pripojenej ku kovovým vodičom alebo bez nej, pričom jednotka využíva digitálne rozhranie termočlánku MAX31855.

„Pridanie nových modelov MKR Shields spoločnosti Arduino do nášho portfólia nám pomáha rozšíriť možnosti dosiek MKR pre našich zákazníkov,“ hovorí Hari Kalyanaraman, globálny riaditeľ divízie jednodoskových počítačov v spoločnosti Farnell. „Vďaka všestrannej kombinácii bezdrôtového pripojenia a možnostiam snímačov poskytuje séria MKR flexibilitu pre technikov a tvorcov, ktorí chcú jednoducho vyvíjať a nasadzovať aplikácie IoT pomocou kompletneho systému Arduino.“

Štyri nové moduly Arduino MKR Shields sú teraz dostupné od spoločnosti Farnell v EMEA, Newark v Severnej Amerike a element14 v APAC.

www.premierfarnell.com



DIGITÁLNY KALIBRAČNÝ CERTIFIKÁT (2)

V predchádzajúcej časti sme sa oboznámili so základnými požiadavkami, ktoré sa kladú na kalibračné certifikáty a ktoré musí spĺňať aj digitálny kalibračný certifikát (DCC).

Štruktúra DCC a príslušné technické riešenia

Výsledkom kalibrácie meradla je zvyčajne vydanie kalibračného certifikátu, ktorý obsahuje informácie o činnosti kalibrovaného meradla. Tieto informácie využíva zákazník, aby zlepšil proces merania kalibrovaným meradlom. Preto logická postupnosť hlavných činností spojených s kalibračným certifikátom zahŕňa:

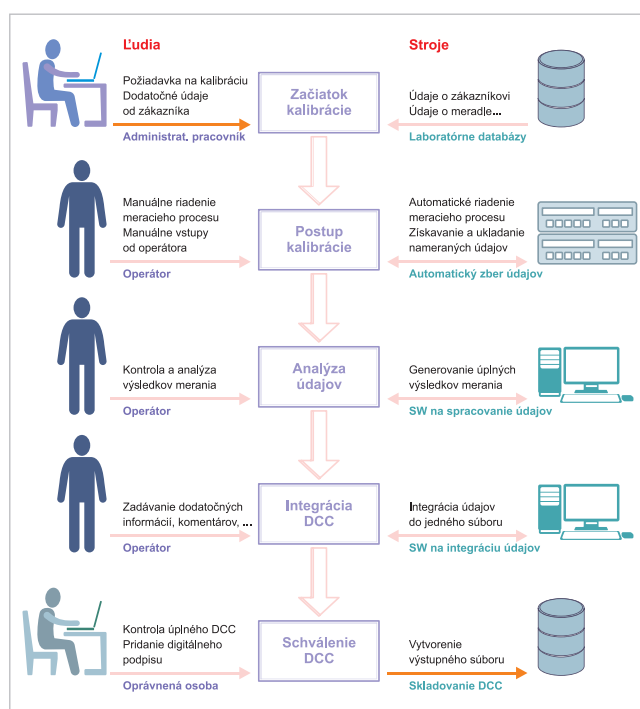
- tvorbu certifikátu,
- jeho doručenie zákazníkovi,
- použitie zákaznikom.

Táto logická postupnosť platí pre tlačný aj digitálny kalibračný certifikát. Samozrejme, aktivity spojené s DCC zahŕňajú niekoľko špecifických prvkov, ktorými sa bude zaoberať nasledujúci text.

Tvorba DCC

Medzinárodné dokumenty (konkrétne [4]) definujú podrobné požiadavky kladené na kalibračný certifikát; preto aj súbor operácií, ktoré sa podieľajú na jeho vytvorení, musí spĺňať tieto požiadavky. Obr. 2 predstavuje schematický pracovný postup s hlavnými činnosťami pri tvorbe DCC. Výsledný certifikát musí spĺňať požiadavky uvedené v časti 4, takže proces tvorby DCC je veľmi komplexnou činnosťou, ktorej výsledkom je výstupný súbor vhodný na ďalšie spracovanie (uloženie, doručenie zákazníkovi atď.).

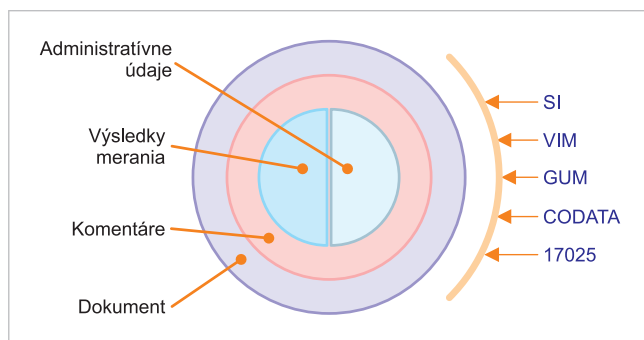
Tvorba DCC zahŕňa viacero krokov, ktoré vyžadujú potrebné vstupy z rôznych zdrojov. Ako znázorňuje obr. 2, tieto vstupy prichádzajú



Obr. 2 Schematický postup vytvárania DCC

typ údajov	obsahuje napríklad tieto body	medzinárodne regulované	záväznosť
administratívne údaje	identifikácia laboratória, identifikácia zákazníka, identifikácia kalibrovaného meradla, identifikácia metódy	regulované	povinné
výsledky merania	hodnoty namerané na etalóne a na kalibrovanom meradle, zodpovedajúca neistota, meracie jednotky	častočne regulované	povinné
komentáre	rôzne vyhlásenia, názory a interpretácie (ak sa požadujú)	neregulované	voliteľné
dokument	náhľad DCC vo formáte .pdf, rôzne jazykové mutácie DCC, dodatkové súbory (video, fotografie, záznamy...)	neregulované	voliteľné

Tab. 4 Prehľad štyroch skupín údajov v DCC



Obr. 3 Hierarchická štruktúra údajov v DCC
(tab. 5 obsahuje vysvetlenie skratiek) (upravené z [5])

bud' z digitálneho prostredia (databázy, meracie a riadiace systémy, softvér na spracovanie dát atď.), alebo od ľudských operátorov (administratívni a laboratórni pracovníci a schvaľovacie orgány).

Podľa [5] obsahuje DCC tieto skupiny údajov:

- administratívne údaje,
- výsledky merania,
- komentáre,
- dokument.

Údaje sú usporiadané v hierarchickej štruktúre (obr. 3). Jadro DCC reprezentujú administratívne údaje a výsledky merania s pripomienkami a ďalšími informáciami uloženými v komplexnom dokumente.

Každá časť má v DCC svoju špecifickú úlohu, pričom využíva rôzne druhy informácií a má na ne aj rôzne požiadavky. Stručný prehľad je uvedený v tab. 4.

Ako znázorňuje obr. 1 (publikovaný v prvej časti seriálu v ATP Journal 6/2019), údaje, ktoré obsahuje DCC, musia spĺňať určité kritériá definované externými dokumentmi. Tieto dokumenty ovplyvňujú obsah kalibračného certifikátu bez ohľadu na jeho formu – vytlačený alebo digitálny (tab. 5).

Administratívne údaje

Táto časť DCC obsahuje najmä údaje na jednoznačnú identifikáciu kalibračného laboratória, kalibračného procesu, zákazníka a kalibrovaného prístroja. Dátové polia určené pre tieto informácie majú pevný formát podľa medzinárodných noriem, obsahujúci písmená v Unicode a arabské číslice. Časť administratívnych údajov v DCC preto spadá do regulovanej oblasti.

Výsledky merania

Patria sem hodnoty namerané počas kalibrácie, analyzované a prezentované vo forme úplného výsledku merania vrátane neistoty merania a príslušných meracích jednotiek, pričom táto časť DCC je čiastočne regulovaná. Úplne regulované sú:

- Štruktúra úplného výsledku merania, ktorý vo všeobecnosti pozostáva z:
 - identifikátora,
 - odhadu nameranej hodnoty,
 - rozšírenej neistoty merania,
 - koefficientu rozšírenia,

skratka	oblasť	odkaz
SI	používanie správnych meracích jednotiek	[6]
VIM	používanie správnej metrologickej terminológie	[3]
GUM	návody na vyhodnotenie neistoty merania	[7]
CODATA	odporúčané hodnoty základných fyzikálnych konštánt	[8]
17025	požiadavky na normalizovaný obsah kalibračného certifikátu	[4]

Tab. 5 Dokumenty definujúce obsah kalibračného certifikátu

- jednotky,
- času (ktorý je nepovinný).

Identifikátory sa uvádzajú vo formáte Unicode, čísla a časové formáty sú definované podľa existujúcich noriem.

- Použitie meracích jednotiek, ako aj ich reprezentácia (pozri [9]). Tento dokument špecifikuje identifikátory jednotiek na podporu počítačového spracovania dát. Poskytuje prehľad množstva so súvisiacimi zbierkami medzinárodne štandardizovaných aj neštandardizovaných jednotiek.
- Postup na vyjadrenie neistoty merania vrátane vyhlásení o faktore pokrytia a predpokladoch.

Neregulovaná je forma, pomocou ktorej sa vyjadruje výsledok kalibrácie. Podľa [3] sa môže kalibrácia vyjadriť „údajmi, kalibračnou funkciou, kalibračným diagramom, kalibračnou krivkou alebo kalibračnou tabuľkou. V niektorých prípadoch môže ísť o aditívnu alebo multiplikatívnu korekciu indikácie s pridruženou neistotou merania.“

Komentáre

Umožňujú poskytnúť ďalšie informácie o získaných výsledkoch merania. Táto časť DCC sa môže použiť podľa potreby a nie je regulovaná. Môžu sa sem vložiť napríklad grafické údaje, video alebo audio informácie, ako aj jednotlivé série meraní v ľubovoľnom formáte.

Dokument

Literatúra [5] predpokladá pri DCC použitie rozšíriteľného značkovacieho jazyka (angl. Extensible Markup Language – XML). XML je jazyk, ktorý definuje množinu pravidiel na kódovanie dokumentov vo formáte, ktorý je čitateľný pre človeka aj pre stroj. XML má viacero výhod, a to najmä:

- široko sa využíva v medzinárodnom meradle ako formát výmeny údajov,
- v súčasnosti už existuje veľké množstvo nástrojov na prácu s XML,
- umožňuje bezpečné použitie kryptografických metód,
- je dobre čitateľný strojmi nezávisle od platformy a je tiež v podstate čitateľný ľuďmi,
- predstavuje formát údajov na dlhodobé ukladanie,
- dá sa ľahko integrovať do databázových aplikácií a internetového prostredia,
- je vhodný na manipuláciu s dátami obsiahnutými v DCC vrátane meracích jednotiek (pozri [9]),
- umožňuje ukladanie voliteľných verzií DCC vo formáte. pdf.

Formát XML sa odporúča aj v [10], čo je dokument, ktorý definuje formát výmeny údajov na riadenie meracích a skúšobných zariadení podporované počítačom.

Doručenie DCC zákazníkovi

Po vytvorení DCC vo forme výstupného súboru ho treba doručiť zákazníkovi. Pri prenose DCC sa musí zabezpečiť integrita a autenticita údajov. Nato sa využívajú kryptografické metódy ochrany informácií.

Priradené v prvom rade sa uvažuje o použití digitálnych podpisov (angl. digital signature – DS) a časových pečiatok. Mnoho krajín na celom svete uznáva používanie digitálneho podpisu na právne účely. Európska únia prijala takzvané nariadenie eIDAS [11] a mnohé členské štáty EÚ prijali aj príslušné právne predpisy.

V dôsledku technického vývoja trvá platnosť DS približne päť rokov. Takže aby sa zaručila čitateľnosť, dostupnosť, integrita a autenticita DCC, musí sa DS pravidelne aktualizovať.

Bez ohľadu na spôsob použitý na pripojenie kryptografických podpisov k DCC je výhodné, ak daný spôsob umožňuje, aby sa jeden alebo viac podpisov pripojilo k jednému DCC, ako aj podpísanie niekoľkých DCC súčasne (hromadný podpis).

Literatúra [11] okrem DS definuje aj používanie elektronických plômb.

Používanie DCC

Používatelia meradiel boli doteraz zvyknutí na tlačene kalibračné certifikáty. Znamená to, že majú postupy na manipuláciu s tlačnými dokumentmi, ich ukladanie, archiváciu atď. Okrem toho výsledky merania obsiahnuté v tlačných kalibračných certifikátoch slúžia ako základ na korekciu výsledkov meraní poskytovaných kalibrovanými meradlami. Tieto korekcie vytvárajú používatelia meradiel a zapisujú sa do softvéru na spracovanie údajov alebo priamo do meradiel. V každom prípade je celý proces pod kontrolou ľudského operátora zodpovedného za správnu implementáciu korekcií.

Teraz je situácia s DCC iná. Používateľ kalibrovaného meradla musí najskôr prijať určité opatrenia na zavedenie príslušnej infraštruktúry IKT. Ide najmä o správu DCC, následnú archiváciu (treba si napríklad uvedomiť, že platnosť digitálneho podpisu trvá približne päť rokov a musí sa pravidelne obnovovať), autorizovaný prístup a manipuláciu s DCC.

Ako už bolo uvedené, jednou z výhod DCC je strojová čitateľnosť obsiahnutých údajov, v tomto prípade výsledkov kalibrácie. Moderné meradlo alebo kontrolný riadiaci systém dokáže automaticky prečítať výsledky kalibrácie a vykonať potrebné korekcie. V princípe sa musí DCC načítať do riadiaceho systému alebo do samotného meradla. Môže to byť citlivá operácia, ktorá by mala byť digitálne zabezpečená, aby sa zabránilo neoprávnenej manipulácii so SW a možnej vírusovej infekcii celého meracieho, resp. riadiaceho systému. Konkrétne sa musí pri určených meradlách zabezpečiť plná dôvera v merací softvér (pozri [12], príloha D Načítanie softvéru pre určené meradlá). Hoci sa táto príručka zameriava na meradlá zahrnuté v smernici MID, výsledky majú všeobecný charakter a môžu sa uplatňovať aj pri meradlách nezahrnutých v smernici MID.

Literatúra

[1] Executive Summary. PTB-Mitteilungen. Heft 4. Metrologie für die Digitalisierung von Wirtschaft und Gesellschaft. [online]. Citované 3. mája 2019. Dostupné na: https://www.ptb.de/cms/fileadmin/internet/publikationen/ptb_mitteilungen/mitt2017/Heft4/PTB-Mitteilungen_2017_Heft_4.pdf.

[2] THIEL, F. – ESCHE, M. – TORO, F. G. – PETERS, D. – OPPERMANN, A. – WETZLICH, J. – DOHLUS, M.: The European Metrology Cloud. [online]. Citované 3. mája 2019. Dostupné na: <https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/>

abteilung_8/8.5_metrologische_informationstechnik/Thiel_OIML_Bulletin_2018_Metrology_Cloud.pdf.

[3] JCGM 200: 2012 International vocabulary of metrology – Basic and general concepts and associated terms (VIM). 3rd edition. 2008 version with minor corrections. [online]. Citované 3. mája 2019. Dostupné na: https://www.bipm.org/utis/common/documents/jcgm/JCGM_200_2012.pdf.

[4] ISO/IEC 17025: 2017 General requirements for the competence of testing and calibration laboratories.

[5] HACKEL, S. – HÄRTIG, F. – HORNIC, J. – WIEDENHÖFER, T.: The Digital Calibration Certificate. [online]. Citované 3. mája 2019. Dostupné na: https://www.ptb.de/cms/fileadmin/internet/publikationen/ptb_mitteilungen/mitt2017/Heft4/PTB-Mitteilungen_2017_Heft_4.pdf.

[6] The International System of Units (SI). [online]. Citované 3. mája 2019. Dostupné na: <https://www.bipm.org/en/measurement-units/>.

[7] JCGM 100: 2008 Evaluation of measurement data – Guide to the expression of uncertainty in measurement. GUM 1995 with minor corrections. [online]. Citované 3. mája 2019. Dostupné na: <https://www.bipm.org/en/publications/guides/gum.html>.

[8] 2010 Recommended Values. [online]. Citované 3. mája 2019. Dostupné na: <http://www.codata.org/committees-and-groups/fundamental-physical-constants/tgfc-previous-values-and-publications>.

[9] IEC TS 62720: 2017 Identification of units of measurement for computer-based processing.

[10] VDI/VDE 2623:2012 Format for data exchange in management of measuring and test equipment. [online]. Citované 3. mája 2019. Dostupné na: <https://www.beuth.de/en/technical-rule/vdi-vde-2623/143033515>.

[11] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. [online]. Citované 3. mája 2019. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[12] WELMEC Guide 7.2, 2018 Software Guide (Measuring Instruments Directive 2014/32/EU1). [online]. Citované 3. mája 2019. Dostupné na: https://www.welmec.org/fileadmin/user_files/publications/WG_07/Guides/WELMEC_Guide_7.2_Software_Guide_2018.pdf.

[13] IEEE 1671-2010 – IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Equipment and Test Information via XML.

[14] Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast). Text with EEA relevance. [online]. Citované 3. mája 2019. Dostupné na: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0032>.

doc. Ing. Martin Halaj, PhD.

Strojnícka fakulta STU v Bratislave
martin.halaj@stuba.sk

UMELÁ INTELIGENCIA PRACOVNÉ MIESTA TVORÍ, NELIKVIDUJE

Montážne roboty, ktoré stavajú veci samy bez toho, aby na to museli byť naprogramované. Samooptimalizujúce sa výrobné linky v továrňach. Vlaky alebo veterné turbíny vyžadujúce údržbu na základe prevádzkových údajov a umelej inteligencie (UI), ktorá dokáže lepšie predpovedať ich správanie ako technici, ktorí ich vyvinuli a vybudovali. Roland Busch, riaditeľ pre technológie v spoločnosti Siemens AG, vysvetľuje, prečo je nepochybné, že UI zmení pracovný trh.

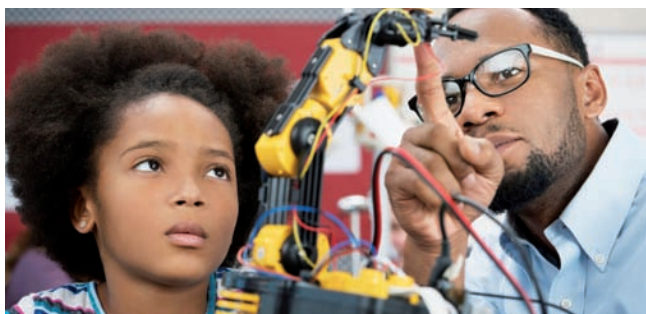
Tento vývoj je príležitosťou v prípade, ak pridáme s nápadmi na jeho pozitívne využitie a pretvorenie UI ako zdroja pracovných miest. Niet pochýb o tom, že čoraz širšie využívanie UI bude meniť svet práce. Vedúce inštitúcie zaoberajúce sa prieskumom trhu sa zhodujú v tom, že až 50 % väčšiny aktivít možno automatizovať. To znamená, že tieto činnosti môžu vykonávať stroje a v skutočnosti ich robia lepšie a rýchlejšie, ako ľudia. To však tiež znamená, že keď sa raz zbavíme týchto podradných úloh, máme viac času na vyhodnotenie dosiahnutých výsledkov, poradenstvo zákazníkom alebo pacientom alebo rozpoznanie a posilnenie schopností našich zamestnancov.



Laboratórium robotiky spoločnosti Siemens v Mníchove. Roboty skladajú produkty bez toho, aby ich predtým niekto naprogramoval.

Dilema „človek verzus stroj“ nie je na mieste

Strachom ovládaná dilema „človek vs stroj“ je zavádzajúca. Tí, ktorí pozorne sledujú tento vývoj, už zaregistrovali iný vývoj. A táto zmena sa už začala. Nemecké priemyselné podniky sa už dnes usilujú o to, aby si navzájom odlákali talentovaných odborníkov, ktorí dokážu prepájať to, čo bolo pôvodne samostatnými disciplínami: špecialisti na spracovanie údajov, ktorí majú tiež znalosti fyziky alebo strojárstva. Iba oni sú schopní prenášať dáta generované umelou inteligenciou napríklad o vlaku do reálneho sveta. Ako príklad možno uviesť situáciu, keď prevádzkovateľ vlaku dostane priamu informáciu o tom, ktorú časť ktorého vlaku treba v konkrétnom čase vymeniť. Táto informácia je výsledkom prediktívnej údržby, analýzy rizík a vedomostí o dostupnosti náhradného dielu a dokonca o právnych podmienkach krajiny, v ktorej sa vlak nachádza. Iba ľudské bytosti majú schopnosť preniesť základné postrehy z digitálneho sveta do reálneho.



Stane sa strachom poznačená debata o nástupe umelej inteligencie minulosťou s príchodom novej generácie?

Z tohto dôvodu sa budeme vždy spoliehať na kvalifikovanú manuálnu prácu, keď sa bude vykonávať na najvyššej úrovni. Vo výrobe a údržbe lokomotív v továrni spoločnosti Siemens v Allachu vykonávajú mechanici a zvárači vysoko presné práce na jednu desatinu milimetra. Dostupnosť vlakov môžeme zaručiť len vtedy, keď túto prácu vykonávajú odborníci.

V súčasnosti prebiehajú tri paralelné zmeny: vznikajú nové pracovné miesta, iné sú menej potrebné, iné sa menia. Aby bol čistý efekt využívania UI pozitívny, komerčné podniky – vrátane veľkých korporácií, malých a stredných podnikov a dokonca aj živnostníkov – musia byť vo všeobecnosti schopné využívať UI. Hovorím tu o priemyselnej UI, čo predstavuje kombináciu UI s vedomosťami o danom odvetví. Naším cieľom je „digitálny spoločník“, ktorý bude zastávať funkciu istého inteligentného pomocníka pre ľudí. Tento druh UI, ktorý podporuje ľudí, musí byť široko dostupný. Nesmieme však len investovať do výskumu a vývoja, ale aj do odbornej prípravy. Navyše tieto zručnosti musia byť podporované aj v predškolských zariadeniach, základných a stredných školách a na univerzitách.

UI môže posunúť Priemysel 4.0 na vyššiu úroveň

Aby súčasná priemyselná revolúcia pokračovala v prospech priemyselných krajín, ako je Nemecko, priemyselné podniky, vládni úradníci, vedci a sociálni partneri musia spoločne budovať iniciatívy podobné úspešnej nemeckej iniciatíve Industrie 4.0. Tento celosvetovo zavedený koncept bude modernizovaný umelou inteligenciou, pretože táto technológia sa bude nachádzať vo všetkom v budúcnosti vrátane IT, výroby, prevádzky priemyselných závodov, samotných produktov a služieb. Priemyselná UI dokáže posunúť Priemysel 4.0 na vyššiu úroveň.

UI bude rozhodujúca pre ďalší rozvoj

Domnievam sa, že v rámci úzkoprísneho, strachom ovplyvneného zmýšľania o umelej inteligencii sa najmä jeden aspekt dostal do úzadia: UI bude rozhodujúca pre ďalší vývoj hrubého domáceho produktu (HDP). Priemerný celosvetový rast vo výške 3,5 % ročne sa v blízkej budúcnosti skončí v dôsledku demografického vývoja. Naše hospodárstvo sa musí transformovať. Dokážeme to s pomocou UI technológií a pracujúceho obyvateľstva, ktorého činnosť nebude primárne pracovne náročná, ale náročná na zručnosti, pričom bude vytvárať hodnotu na základe kvalifikácie a produktivity.

Krajiny alebo spoločnosti, ktoré si želajú uspieť v dnešnom svete, musia svoje hospodárstvo prispôsobiť budúcnosti. Vedúci výskumníci na trhu sa zhodujú v názore, že UI technológia – správne a dôsledne nasadzovaná – má potenciál zvýšiť hrubý domáci produkt ekonomík, ako je Nemecko. Úspešne sme začali digitálnu transformáciu s Priemyslom 4.0. S priemyselnou UI môžeme teraz prejsť na úplne novú úroveň.

Zdroj: Busch, R.: AI is Job Negine, not a Job Killer. [online]. Siemens AG. Publikované 27. 7. 2018.

-tog-

METÓDY STROJOVÉHO UČENIA V SLUŽBÁCH KYBERNETICKEJ BEZPEČNOSTI CAV (1)

Článok je zamyslením autorov nad aktuálnymi výzvami, ktoré sa vynárajú v oblasti kybernetickej bezpečnosti automobilových aplikácií v súvislosti s prepojenými a autonómnymi vozidlami, a nad tým, akú úlohu zohrávajú alebo môžu zohrávať metódy strojového učenia v celom procese. Obsahuje prehľad súčasného stavu a poukazuje na existujúce problémy, najmä bezpečnostné a potenciál vybraných metód.

Spomedzi nepreberného množstva existujúcich definícií umelej inteligencie (UI) môžeme vybrať tú, ktorá hovorí, že ide o schopnosť digitálneho počítača alebo počítačom riadeného robota vykonávať úlohy bežne spájané s inteligentnými bytosťami. Tento pojem sa často používa pri vývoji systémov zahŕňajúcich intelektuálne procesy charakteristické pre človeka, ako je jeho schopnosť usudzovať, objavovať zmysel niečoho, zovšeobecňovať alebo učiť sa z minulých skúseností.

S určitými formami UI sa už (často nevedomky) stretávame pri používaní našich mobilov, obsluhu inteligentných (smart) systémov a zariadení, práci na internete a pod. Ide o aplikácie inteligentných algoritmov zamerané na pokročilé spracovanie dát, optimalizáciu procesov, inteligentné rozhodovanie a riadenie a pod., ktoré majú ďaleko predstavám tvorcov sci-fi žánru. Dosiahnutie tzv. nadľudskej inteligencie alebo superinteligencie je jedným z vedeckých snov ľudstva, ku ktorému súčasný výskum iba hľadá cesty [1]: emulácia činnosti ľudského mozgu, zdokonaľovanie činnosti biologických mozgov, tvorba rozhrania mozog – počítač, prechod od individuálnej ku kolektívnej (sieťovej) inteligencii či rozvoj samotného odvetvia UI, ktorý je v súčasnosti výrazne poháňaný najmä priemyslom a čelí dvom technologickým mega trendom – globálnemu prepojeniu sveta a dynamickému vývoju technológií UI. Všetky prístupy skôr či neskôr nastolia aj množstvo etických, právnych či ešte netušených typov problémov, s ktorými sa bude potrebné vyrovnávať. Stretnúť sa možno s rôznymi koncepciami uvažujúcimi o možnostiach budúceho vývoja UI.

Najčastejšie sa skloňujú tri formy UI [2]:

- UI úzka alebo slabá (ANI – Artificial Narrow Intelligence): úzko špecializovaná na jedinú oblasť;
- UI všeobecná, silná alebo na ľudskej úrovni (AGI – Artificial General Intelligence, Strong AI, Human-Level AI): s počítačmi inteligentnými tak ako ľudia;
- umelá superinteligencia (ASI – Artificial Superintelligence): na základe definície Nicka Bostroma je oveľa múdrejšia ako najlepší ľudský mozog prakticky v každej oblasti vrátane vedeckej tvorivosti, všeobecnej múdrosti a sociálnych zručností.

Iná koncepcia hovorí o troch vlnách – vlne expertných systémov, vlne štatistického alebo strojového učenia a budúcej vlne spájajúcej predošlé dve s cieľom dosiahnuť kontextovú sofistikovanosť, abstrakciu a vysvetlenie. Najviditeľnejšou a médiami pravdepodobne najsledovanejšou oblasťou je vývoj prepojených a autonómnych vozidiel (Connected and Autonomous Vehicles – CAV), ktorý nám najlepšie nastavuje zrkadlo súčasného stavu a (ne)dokonalosti súčasnej úrovne UI. Samostatne jazdiace automatizované vozidlá sú odrazom druhej vlny v zmysle spomenutej koncepcie. Technológie nám zatiaľ slúžia na zdokonalenie našich fyzických a psychických daností – rýchlosť, presnosť, opakovateľnosť a pod., neexistuje však nič, čo by človek nevedel robiť a stroj áno. Absencia tzv. zdravého rozumu (Common sense) stále robí zo strojov iba našich pomocníkov a zanecháva nás na úrovni slabej UI. Už aj táto úroveň je však dostatočná na to, aby nám predostierala niektoré neprijemné otázky a problémy, ktorých riešenie vyvolá vrásky odborníkov z viacerých oblastí.

Ako bude uvedené v ďalšom texte, vývoj CAV je toho najlepším dôkazom. Najviac problémov sa vynára v súvislosti s dosiahnutím

požadovanej úrovne bezpečnosti vyvíjaných inteligentných technológií – bezpečnosti v zmysle obidvoch anglických výrazov safety aj security. Ide o oblasť, ktorej dlhodobu nebola venovaná primeraná bezpečnosť a s narastajúcou úrovňou zložitosti, konektivity a dostupného výpočtového výkonu je prítomná čoraz intenzívnejšie.

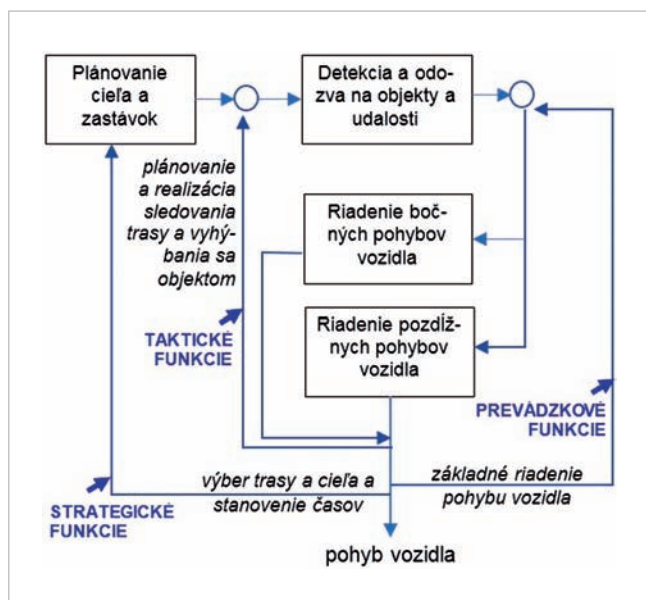
V súvislosti s rizikami implementácie prístupov UI sa odborná verejnosť delí na tri názorové prúdy zastávajúce nasledujúce stanoviská [5]:

- Techno-skeptici: „Nemali by sme sa báť, pretože v dohľadnej budúcnosti UI nedosiahne úroveň ľudí (najmenej stovky rokov).“
- Digitálni utopisti: „Nemali by sme sa báť – dôjde k tomu (možno čoskoro), ale je prakticky zaručené, že to bude dobrá vec (digitálny život je prirodzený a žiaduci ďalší krok v našom kozmickom vývoji).“
- Členovia hnutí hovoriacich o úžitku UI: „Záujem je opodstatnený a užitočný, pretože výskum a diskusia o bezpečnosti UI teraz zvyšuje šance na dobrý výsledok (cieľom by malo byť vytvorenie užitočnej inteligencie).“

Akademické kruhy sú takisto rozdelené – jeden názor predstavuje UI ako existenčnú hrozbu pre ľudstvo, prínosy by však mali prevážiť náklady; druhý názor kladie do centra pozornosti otázku spravodlivosti, zodpovednosti a transparentnosti vývoja UI. Na čom sa však odborníci na bezpečnosť už teraz vedľa rámcovo zhodnúť, je skutočnosť, že preukázať bezpečnosť technológií obsahujúcich UI bude veľmi zložitý problém, čo vyplýva zo samotnej jej podstaty. Štandardne by bolo napr. potrebné poskytnúť presnú, úplnú a jednoznačnú špecifikáciu funkčného správania technického systému, čo sa pri predstave zakomponovania napr. stále sa učiacich (a teda nepretržite sa vyvíjajúcich) technológií dá len ťažko predstaviť. Navyše pri posudzovaní bezpečnostného dosahu UI treba mať na pamäti možnosť jej zneužitia a/alebo jej nedokonalosti. V druhom prípade môže byť cieľ UI ušľachtilý, vzhľadom na nedokonalosť však môžu byť metódy zvolené na jeho dosiahnutie devastácie. Stačí si predstaviť riešenie environmentálnych problémov Zeme, kde by najefektívnejším spôsobom pre UI bolo „odstránenie ľudstva“ ako najväčšieho pôvodcu znečistenia a ekologických problémov. Ukazuje sa, že Asimovove zákony nie sú pre bezpečnú koexistenciu človeka s inteligentnými strojmi dostatočné a do popredia sa skôr dostávajú princípy iniciatívy [3], ktoré sú o to naliehavejšie, o čo sú jednotlivé výskumné oblasti rozdrobenejšie a neschopné vzájomnej spolupráce a integrácie.

Automatizácia CAV

Automatizácia prepojených a/alebo autonómnych vozidiel (CAV) je oblasťou, kde sa automobilový priemysel snaží nasadzovať najnovšie technologické riešenia vrátane implementácie metód a algoritmov UI. Riešenia smerujú okrem samotného výrobného procesu k zvýšeniu úrovne asistencie a/alebo automatizácie počas vedenia vozidiel, ich prepojitelnosti vrátane využívania služieb cloudových platforiem, k vývoju nových aplikácií pre oblasť poisťovníctva a likvidácie škodových udalostí, sledovaniu vitálnych funkcií vodiča



Obr. 1 Úloha dynamického riadenia [4]

automatizácia	vodič	monitoring
0	iba vodič	monitorované riadenie
1	vodič s pomocou	
2	ruky dočasne mimo volantu	
3	podmienená automatizácia	nemonitorované riadenie
4	vysoká automatizácia	
5	plná automatizácia	

Tab. 1 Úrovně automatizácie riadenia vozidla podľa [4]

a/alebo ďalších členov osádky a pod. Z hľadiska procesu vedenia vozidla a jeho automatizácie vstupujú do procesu riadenia tri primárne faktory – vodič, systém riadenia vozidla a ďalšie systémy a komponenty vozidla, ktoré pri uvažovaní prostredia realizujú úlohu dynamického riadenia (obr. 1).

Všeobecne akceptovaný dokument [4] zdefinoval päť úrovní automatizácie (tab. 1), pričom na trhu už sú k dispozícii úrovne 0 až 3, vyššie stupne sú v procese testovania. Kategorizácia je založená na posúdení:

- či systém automatizácie riadenia vozidla realizuje podúlohy bočného a pozdĺžneho pohybu v úlohe dynamického riadenia,
- či systém automatizácie riadenia vozidla realizuje podúlohy bočného a pozdĺžneho pohybu v úlohe dynamického riadenia súčasne,
- či systém automatizácie riadenia vozidla tiež realizuje podúlohu detekcie a reakcie na objekty a udalosti,
- či systém automatizácie riadenia vozidla tiež realizuje odovzdanie úlohy dynamického riadenia,
- či je systém automatizácie riadenia vozidla limitovaný návrhom operačného prostredia.

V úrovni 0 má vodič výhradnú kontrolu nad svojím vozidlom, aj keď môžu existovať systémy aktívnej podpory (napr. parkovacie senzory, tempomat na udržiavanie rýchlosti). Úroveň 1 obsahuje asistenčné systémy umožňujúce vozidlu čiastočne reagovať na podnety z okolia (napr. adaptívny tempomat či systém na udržiavanie vozidla v jazdnom pruhu). Realizujú sa podúlohy bočného alebo pozdĺžneho riadenia, nie však obidve súčasne (príklad: 2018 Honda Civic). Úroveň 2 využíva prepojenie technológií prvej úrovne, vďaka čomu je vozidlo schopné na obmedzený čas prebrať úplnú kontrolu nad rýchlosťou a riadením, pri riešení problémov sú však zásahy vodiča nevyhnutné (príklad: 2018 Tesla Model S). V úrovni 3 je vozidlo schopné pri zadaní trasy nahradiť vodiča, v prípade problémov však musí dôjsť k okamžitému odovzdaniu riadenia naspäť vodičovi, čo je hlavná slabina a nebezpečný aspekt tohto konceptu (príklad: 2019 Audi 8). V úrovni 4 sa vyžaduje zásah vodiča iba v kritických

situáciách, zväčša po predošlom automatizovanom zastavení (príklad: Hyundai NEXO – v rámci testovania). Všetky úrovne 1 až 4 sa odohrávajú v obmedzenom operačnom prostredí. Najvyššia úroveň 5 zodpovedá plne autonómnemu vozidlu, ktoré sa pohybuje v ľubovoľnom prostredí a nepredpokladá zásahy vodiča (preto v princípe nemusia ani existovať ovládacie prvky – volant, pedále a pod.). Jej dosiahnutie predpokladá zvládnutie troch základných prekážok – videnie, vnímanie (vrátane porozumenia videného) a konanie.

Vzhľadom na nedokonalosť senzorov musia byť využívané viaceré detekčné princípy, ktorých výstupy sa prekrývajú a dopĺňajú. Snímané dáta musia byť správne interpretované s cieľom v reálnom čase detegovať stacionárne aj pohyblivé objekty v danom prostredí. Zohľadňovať sa musia dopravné podmienky, výskyt chodcov, poveternostné podmienky, stav vozovky, komunikácia s ostatnými subjektmi (V2X) atď. Najťažšou úlohou je prijímať bezpečné rozhodnutia, čo vyžaduje otestovať a vyhodnotiť miliardy možných aj nepravdepodobných scenárov.

V rámci jednotlivých podúloh úlohy dynamického riadenia možno identifikovať rôzne prístupy – od klasických (nevyužívajúcich metódy UI) cez prístupy opierajúce sa o implementáciu UI algoritmov až po kombináciu oboch prístupov.

Problémy bezpečnosti CAV

Legislatívny rámec

Naliehavé výzvy prichádzajúce s digitalizáciou nášho životného priestoru nevynechávajú ani automobilový priemysel. V snahe napomôcť rozvoju autonómnej mobility prijala Európska komisia (EK) stratégiu [5], ktorá vytvára rámec pre ďalší vývoj v zmysle vyššie uvedených skutočností. Okrem funkčnej a technickej bezpečnosti (safety) sa do popredia dostávajú aj otázky bezpečnosti fyzickej, informačnej, kybernetickej (security).

Požiadavky na funkčnú bezpečnosť cestných vozidiel sa definujú v zmysle ISO 26262 – Functional Safety for Road Vehicles, ktorá vychádza zo všeobecne známej IEC 61508 a predstavuje jej aplikáciu v oblasti automotive aplikácií s vysokou integritou. Znamená to, že musia byť stanovené dodatočné požiadavky na vývojový proces. Okrem rozsiahleho a systematického overovania, validácie a testovania s príslušnou dokumentáciou o každom kroku vývojového procesu musia inžinieri preukázať celkovú zhodu s normou pomocou dokumentu opisujúceho, ako každý krok v životnom cykle vývoja spĺňa príslušné požiadavky normy. Takisto treba preukázať, že nástroje použité na vývoj sú pre dané úlohy vhodné. Norma definuje funkčnú bezpečnosť ako „neprítomnosť neprimeraného rizika v dôsledku nebezpečenstva spôsobeného nesprávnym správaním elektrických alebo elektronických systémov“. Možno ju aplikovať na SW alebo HW komponenty alebo ich kombináciu. Pracuje sa „automobilovými úrovňami integrity bezpečnosti“ (Automotive Safety Integrity Level – ASIL), ktoré možno jednoducho vyjadriť ako súčin:

$$ASIL = \text{závažnosť} \times (\text{expozícia} \times \text{riaditeľnosť}) \quad (1)$$

kde:

- **závažnosť (Severity):** vážnosť alebo intenzita poškodenia alebo následkov s ohľadom na život ľudí v prípade porušenia bezpečnostných cieľov (S1 – slabé a stredné zranenia, S2 – vážne zranenia a zranenia ohrozujúce život, S3 – zranenia vedúce k úmrtiu);
- **expozícia (Exposure):** kvantifikácia možnosti, že sa vozidlo ocitne v nebezpečnej alebo rizikovej situácii, ktorá môže spôsobiť škody na zdraví ľudí a majetku (E1 – veľmi malá pravdepodobnosť, E2 – malá pravdepodobnosť, E3 – stredná pravdepodobnosť, E4 – vysoká pravdepodobnosť);
- **riaditeľnosť (Controllability):** rozsah, v rámci ktorého je vodič schopný zvládnuť (riadiť) vozidlo, ak dôjde k porušeniu bezpečnostného cieľa v dôsledku zlyhania alebo nesprávneho fungovania akéhokoľvek vyhodnocovaného komponentu vozidla ($C1 < C2 < C3$, kde C1 je ľahká riaditeľnosť a C3 je obťažná riaditeľnosť).

Výsledkom sú štyri úrovne A, B, C, D priradené na základe alokácie tabuľky (tab. 2). Kombinácia S3, E4 a C3 reprezentuje vysoko nebezpečnú situáciu, naopak S1, E1 a C1 zodpovedá najnižšej úrovni

	trieda pravdepodobnosti	trieda riaditeľnosti		
		C1	C2	C3
trieda závažnosti	S1	E1	QM	QM
		E2	QM	QM
		E3	QM	A
		E4	QM	B
	S2	E1	QM	QM
		E2	QM	QM
		E3	QM	A
		E4	A	B
	S3	E1	QM	QM
		E2	QM	A
		E3	A	B
		E4	B	C

Tab. 2 Alokačná tabuľka podľa ISO 26262

integrity bezpečnosti, ktorá hovorí, že prípadné zlyhanie komponentu nie je nebezpečné, a teda nevyžaduje žiadne dodatočné opatrenia v zmysle ISO 26262. V tabuľke je označená ako úroveň QM (Quality Management Level). Ako typické príklady jednotlivých úrovní možno uviesť napr. zlyhanie rádia (QM), zlyhanie obidvoch zadných alebo obidvoch brzdových svetiel (ASIL-A), zlyhanie obidvoch predných svetiel alebo neplatné údaje zo zadnej kamery (ASIL-B), mimovoľné brzdenie (ASIL-C), nechcená akcelerácia (ASIL-C až D), ovládanie volantu alebo nežiaduce plné brzdenie ABS, neúmyselná aktivácia airbagov (ASIL-D). Približné vyjadrenie vzťahu úrovní ASIL a úrovní integrity bezpečnosti definované inými normami je v tab. 3.

aplikačná doména	úrovně integrity bezpečnosti				
automotive (ISO 26262)	QM	ASIL-A	ASIL-B	ASIL-C	ASIL-D
všeobecné (STN EN 61508)	–	SIL-1	SIL-2	SIL-3	SIL-4
letectvo (ED-12/DO-178/DO-254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
železnica (STN EN 50126/50128/50129)	–	SIL-1	SIL-2	SIL-3	SIL-4

Tab. 3 Približné porovnanie úrovni integrity bezpečnosti v rôznych aplikačných oblastiach

Pretože ide o kvalitatívny koncept, úrovne ASIL majú skôr informatívny charakter – ich klasifikácia závisí do značnej miery od kontextu a interpretácie. Na kvantifikáciu bezpečnostných požiadaviek používa ISO 26262 rôzne metriky – Failures in Time (FIT), Single Point Fault Metric (SPFM), Latent Fault Metric (LFM). Do budúcnosti možno očakávať redefiníciu parametra „riaditeľnosti“, pretože súčasná definícia hovorí o ľudskom vodičovi a jeho neprítomnosť by znamenala v autonómnych vozidlách automaticky úroveň C3 (extrém „neriaditeľnosti“). Zvyšné dva parametre zostanú s najvyššou pravdepodobnosťou bez zmeny. ISO 26262 poskytuje požiadavky na činnosti a metódy, ktoré by bolo potrebné zobrať do úvahy v procese dosahovania funkčnej bezpečnosti, nepredstavuje však návod na to, ako by tieto požiadavky mali byť splnené. Informácie o ďalších dokumentoch súvisiacich s relevantnou štandardizáciou (pohľad U.S. DoT k 08/2018) možno nájsť napr. v [6].

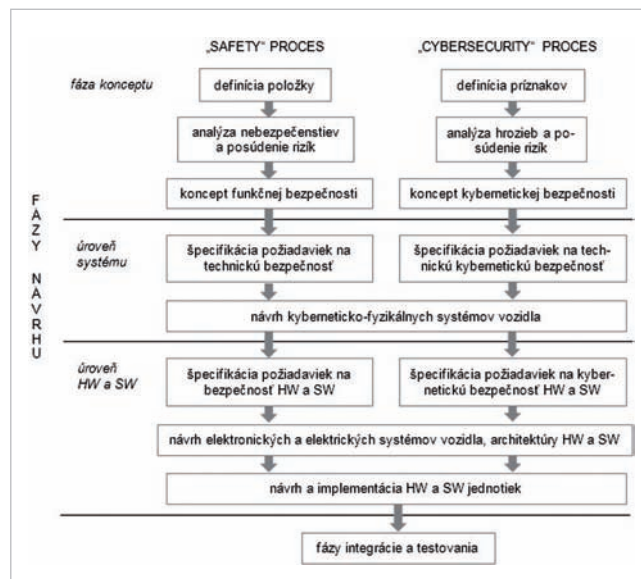
Zlyhanie automobilových komponentov, ktoré neplnia alebo plnia viac alebo menej závažné bezpečnostné ciele, môže byť spôsobené aj externými vplyvmi – či už zamýšľanými, alebo náhodnými. Problematika kybernetickej bezpečnosti v súvislosti s CAV sa dostáva do popredia s nárastom nových hrozieb kybernetických útokov vyplývajúcich z prepojitelnosti vozidiel a systémovej integrácie tisícok komponentov [5]. Podľa [7] bude 75 % z celkového počtu 92 mil. automobilov celosvetovo predaných v roku 2020 pripojených na internet. V súčasnosti neexistuje odvetvový prístup

k ochrane vozidla pred kybernetickými útokmi. Preto EK prijala v roku 2017 balík opatrení v oblasti kybernetickej bezpečnosti [8], uverejnila usmernenia týkajúce sa bezpečnostnej a certifikačnej politiky potrebné na bezpečnú a dôveryhodnú komunikáciu správ súvisiacich s bezpečnosťou cestnej premávky a riadením dopravy medzi vozidlami a infraštruktúrou [9] a uznesením A8-0036/18/P8_TA-PROV(2018)0063 ju Európsky parlament zaviazal zverejniť legislatívny návrh na zabezpečenie rovnakých podmienok na prístup k palubným údajom a zdrojom, ktoré majú obrovský potenciál na vytváranie nových a personalizovaných služieb a výrobkov (pomoc, poistenie, oprava, prenájom, represia a pod.). V zámorí bol iniciovaný a neskôr reiniciovaný obdobný proces (tzv. Security and Privacy in Your Car (SPY) Car Act of 2015, 2017), ktorý zatiaľ viedol k publikovaniu návodov [10] a osvedčených postupov [11] pre aplikácie v Spojených štátoch.

V rámci vytváraného legislatívneho a štandardizačného procesu však existujú viaceré základné dilemy [7], predovšetkým:

- kto je (bude) vlastníkom dát zbieraných z vozidla?
- ide o osobné dáta?
- kto zodpovedá za ich bezpečnosť?
- komu k nim umožniť prístup?
- aká je úloha štandardov a relevantných organizácií?

Funkčná a prevádzková bezpečnosť prepojených a autonómnych vozidiel je predmetom dlhodobého výskumu. Zložitý kyberneticko-fyzikálne systémy v ňom (okrem fyzickej infraštruktúry a fyzických vozidlových systémov) začínajú hrať čoraz dôležitejšiu úlohu. Z hľadiska vývojového procesu nie je kybernetická bezpečnosť iba jedným komponentom navyše, musí byť integrálnou súčasťou fázy plánovania, od samotného konceptu cez výrobu, prevádzku a údržbu až po vyradenie systému z činnosti, ako je zjednodušene naznačené na obr. 2 [12]. Oblasť kybernetickej bezpečnosti riadi najmä ISO 21434, problematiku ochrany údajov ISO 27001 a mnohé ďalšie.



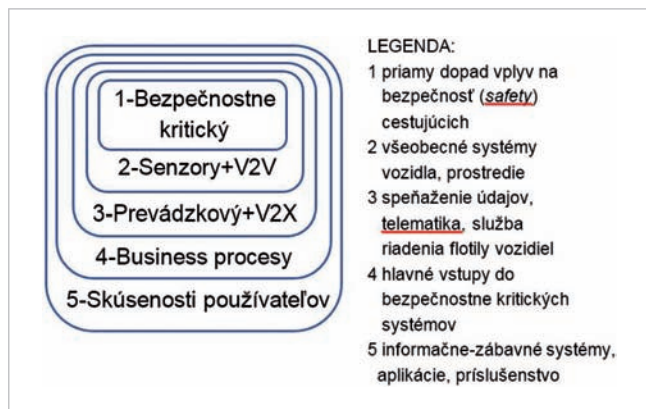
Obr. 2 Safety a security v návrhu systémov autonómnych inteligentných vozidiel a inteligentnej infraštruktúry [12]

Prečo by mal rásť náš záujem o bezpečnosť?

Dostupné štatistiky jednoznačne preukazujú prudký nárast bezpečnostných incidentov. Podľa [13] v prvom kvartáli 2019 bolo identifikovaných 51 incidentov, čo je v porovnaní s rovnakým obdobím minulého roku (15 incidentov) viac ako 300 % nárast (za celé obdobie 2018 išlo o 66 incidentov). Berúc do úvahy posledný prieskum spoločnosti Cisco, existuje analógia s viac ako 350 % celoročným nárastom ďalšieho javu v kybernetickom priestore známeho ako ransomware. V niektorých prípadoch bol cieľom tohto typu útoku už aj automobilový sektor. V rámci rozdelenia hackerov na etických (tzv. white hat) a „zlých“ (tzv. black hat) v prvom štvrtroku 2019 narástol ich percentuálny pomer z 45/55 na 28/72 v prospech black hat hackerov, čo je dôkazom rastúcej miery rizika. Prehľad cieľov najčastejších vektorov útoku je v tab. 4.

systém bezklúčového vstupu	47 %
servery	17 %
mobilné aplikácie	6 %
zbernica CAN (Controller Area Bus)	4 %
ECU (Engine Control Unit)	4 %
Infotainment (informačno-zábavný systém)	4 %
port OBD (On-board Diagnostics)	4 %
Bluetooth	2 %

Tab. 4 Najčastejšie vektory útoku v 1. kvartáli 2019 [13]



Obr. 3 Dekompozícia ekosystému prepojeného vozidla na päť vzájomne spojených podsystémov [15]

Štatistické údaje z rovnakého zdroja hovoriace o motivácii útokov uvádzajú snahu o odcudzenie vozidla (40 %), narušenie/poškodenie aktivít súvisiacich s podnikaním a poskytovaním služieb (17 %), získanie kontroly nad vozidlom (14 %), porušenie údajov (10 %) či snahu o realizáciu podvodných aktivít (5 %).

Predikcie na rok 2019 nie sú o nič optimistickéjšie [14]:

- s každou novou službou nový vektor útoku,
- narušení ochrany osobných údajov výmenou/zdieľaním vozidiel,
- nárast a zdokonaľovanie hackerských útokov na autonómne senzory,
- nárast počtu podvodov a zneužitia v oblasti smart mobility,
- nárast útokov na bezklúčový vstup do vozidla,
- potenciálna možnosť útoku na celú flotilu vozidiel.

Hrozby v oblasti kybernetickej bezpečnosti v ostatných rokoch výrazne menia svoj charakter [16]:

- zmena motivácie útočníka – motivácia môže byť rôznorodá (ideologické dôvody, snaha ukázať prevahu, nespokojnosť, donútenie, náhoda, osobné uspokojenie, závislosť, zvedavosť, finančný profit apod.); principiálne dochádza k posunu od jednotlivca poháňaného motívom zvedavosti k útokom dobre financovaných a vyškolených útočníkov v rámci kybernetickej vojny alebo sofistikovaných aktivít kriminálnych organizácií;
- nárast rýchlosti a šírky záberu útokov – od ručného nájdenia slabého miesta softvéru na konkrétnom počítači sa prechádza k automatizovanému vyhľadávaniu slabých miest, ich šíreniu cez internet a globálnemu ovplyvňovaniu všetkých pripojených zariadení;
- podstatný nárast potenciálneho dosahu narušenia – globálne prepojenie zariadení a ľudí znamená, že útoky neovplyvnia iba digitálny svet (ako v minulosti), ale tiež fyzický svet prostredníctvom internetu vecí a sveta spoločnosti cez všadeprítomné platformy sociálnych médií.

Literatúra

- [1] BOSTROM, N.: Superintelligence. Paths, Dangers, Strategies. Oxford University Press 2014. ISBN 978-0-19-967811-2.
- [2] URBAN, T.: The AI Revolution: The Road to superintelligence. Wait But Why? [online]. Dostupné na: <https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html>.

[3] Asilomar AI Principles. [online]. Dostupné na: <https://futureoffi-fe.org/ai-principles/?submitted=1#confirmation>.

[4] SAE J3016TM Levels of Driving Automation. SAE International, 2018.

[5] COM (2018) 283 final: Na ceste k automatizovanej mobilite: stratégia EÚ pre mobilitu budúcnosti. Oznámenie komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru, výboru regiónov, 2018.

[6] Preparing for the future of transportation. Automated vehicles 3.0. U. S. Department of Transportation, October 2018.

[7] The state of security regulation in the connected car ecosystem. Challenges, dilemmas and stakeholders' interests. E-book, Upstream Security Ltd. 2018.

[8] Digital Single Market. Policy. Cybersecurity. EK, 2018. Dostupné na: <https://ec.europa.eu/digital-single-market/en/cyber-security>.

[9] Intelligent Transport Systems: Cooperative, connected and automated mobility (CCAM). EK 2019. Dostupné na: https://ec.europa.eu/transport/themes/its/c-its_en.

[10] Accelerating the Next Revolution in Roadway Safety. Federal Automated Vehicles Policy. NHTSA, Septembre 2016.

[11] Cybersecurity best practices for modern vehicles. Report No. DOT HS 812 333, NHTSA, October 2016.

[12] TOKODY, D. et al.: Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. Interdisciplinary Description of Complex Systems, 16(3-A), 384-396, 2018.

[13] Q1 2019 sees rapid growth of automotive cyber incidents. Upstream Security Ltd. 2019.

[14] Upstream security global automotive cybersecurity report 2019. Research into smart mobility cyber attacks trends. Upstream Security Ltd. 2019.

[15] GOLDBERG, J.: Traditional IT Cyber Security vs. Automotive Cyber Security Explained. Guard Knox, March 2018.

[16] Artificial Intelligence and Machine Learning Applied to Cybersecurity. The results of an intensive three-day IEEE Confluence. IEEE, 6-8 October 2017.

[21] APRUZZESE, G. et al.: On the Effectiveness of Machine and Deep Learning for Cyber Security. 10th Int. Conference on Cyber Conflict (CyCon), IEEE 2018.

[22] PANIMALAR, A. S. et al.: Artificial Intelligence Techniques for Cyber Security. In: International Research Journal of Engineering and Technology (IRJET), 2018, Vol. 5, Iss. 3.

[23] GREGOR, M. – JANOTA, A. – HRUBOŠ, M.: Kompendium vybraných metód umelej inteligencie 1. VŠ učebnica, Žilinská univerzita v Žiline, 2018. 211 s.

[24] CHOCKALINGAM, S. et al.: Bayesian Network Models in Cyber Security: A Systematic Reviews. Proc. of the Nordic Conference on Secure IT Systems (Nordic 2017), TU Delft, 2017.

Pokračovanie v ďalšom čísle.

prof. Ing. Aleš Janota, PhD., Eurling
ales.janota@fel.uniza.sk

Ing. Roman Michalík
roman.michalik@fel.uniza.sk

Žilinská univerzita
Fakulta elektrotechniky a informačných technológií
Katedra riadiacich a informačných systémov
Univerzitná 1, 010 26 Žilina
Tel.: +421 41 513 3356

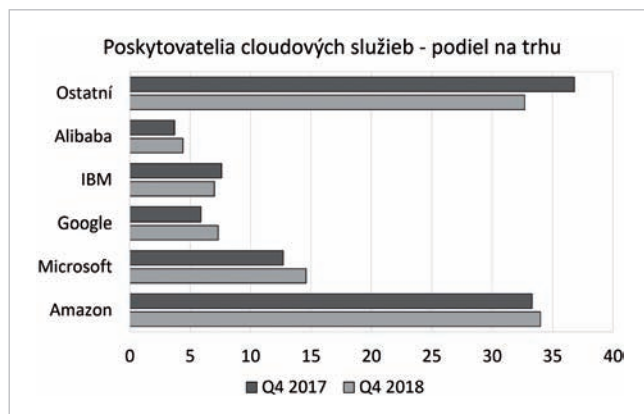
SMART/INTELLIGENT EDGE – POSKYTOVATELIA PLATFORIEM CLOUD A EDGE

V predchádzajúcej časti série Smart/Intelligent edge [1] sme sa venovali analýze hardvéru potrebného na implementáciu inteligentných brán a riešení na hrane siete v závislosti od ich typu [2] a očakávanej úlohy na hrane siete. Na týchto zariadeniach sú spustené rôzne algoritmy podľa charakteru riešenia na hrane siete, ktoré sme opísali v predchádzajúcich dieloch [3], [4]. Táto časť sa bude venovať práve veľkým poskytovateľom cloudových platforiem. Ak chcete dnes implementovať riešenie na hrane siete, nie je nutné zakúpiť si celé aplikácie alebo zaplatiť programátora či integrátora. Stačí, ak si zakúpite takéto riešenie ako službu a cloudový poskytovateľ vám dodá potrebné inštalračné balíky a inštrukcie k nasadeniu časti inteligencie na hrane siete.

Na aplikáciu edge technológií prichádzajú do úvahy aj otvorené riešenia (open source). Ak si ich však vyberiete, nevyhnete sa programovaniu, nakoľko tieto kódy treba zväčša modifikovať s ohľadom na konkrétne riešenie. Práve preto možnosti predpripravených balíčkov od cloudového poskytovateľa sa javia ako jednoduchšia a rýchlejšia možnosť nasadenia.

Najväčší poskytovatelia cloudových služieb

Najväčší dodávatelia cloudových služieb sa postupne stávajú aj najväčšími poskytovateľmi riešení pre hranu siete. Podľa [5] (obr. 1) sú nimi dnes Amazon (Amazon Web Services – AWS), Microsoft (Azure), Google (Google Cloud Platform) a IBM (IBM Cloud, predtým Bluemix). Tieto štyri spoločnosti sú na vrchných priečkach, odkedy predstavili svoje cloudové platformy. Za posledné roky sa udiala len jedna zmena, a to tá, že Google sa dostal nad IBM a že už aj na tieto firmy sa začína doťahovať konkurencia (Alibaba, AT&T a ďalšie spoločnosti).

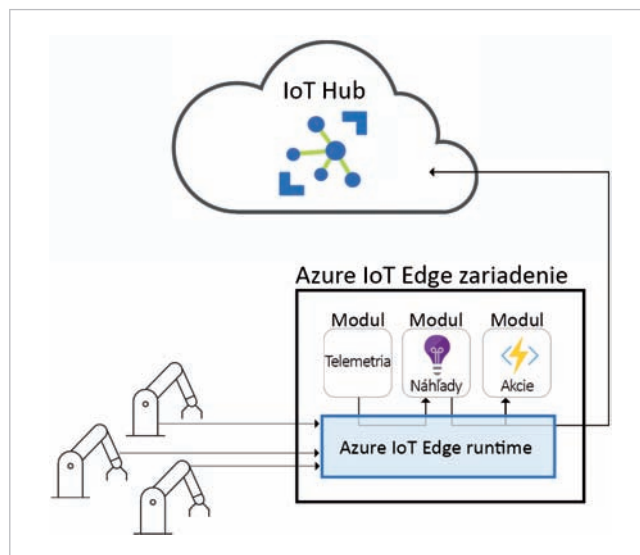


Obr. 1 Najväčší dodávatelia cloudových služieb [5]

Microsoft Azure

Poskytovanie služieb na hrane siete najďalej posunul Microsoft, kde si môžete vybrať služby, ktoré sa priamo spájajú s klasickými cloudovými službami ako IoT Hub (služba na pripojenie IoT zariadení), Stream Analytics (predspracovanie a príprava dát), Storage (úložisko), DocumentDB (NoSQL databáza), Power BI (analytický nástroj) a mnoho ďalších. Na obr. 2 môžete vidieť jedno z takýchto riešení Microsoft Azure IoT Edge.

Najskôr potrebujete na edge zariadenie nainštalovať operačný systém s linuxovým jadrom a Dockerom. Na toto zariadenie sa pomocou vzdialeného prístupu (SSH) prihlásite v konzole portálu



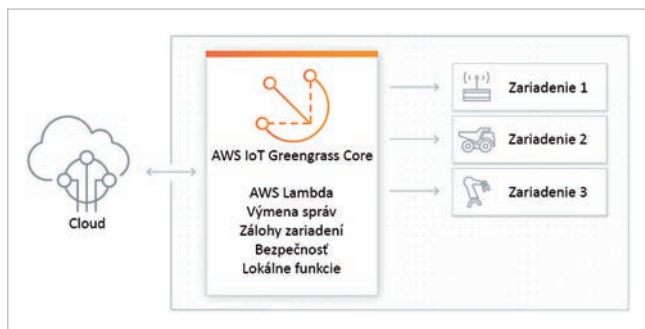
Obr. 2 Microsoft Azure IoT Edge [6]

Azure. Potom už môžete vybrať a konfigurovať vhodné služby pre riešenie, akoby ste si kupovali služby na cloude. Jednotlivé služby sa inštalujú priamo do jednotlivých kontajnerov v Dockeri. Služby sú spoplatnené podľa cenníka na základe počtu a objemu transakcií (niektoré služby sú aj zadarmo).

Amazon Web Services

Amazon ponúka službu AWS IoT Greengrass, ktorá prináša lokálne výpočty, možnosti posielania správ, ukladania údajov do dočasnej pamäte, synchronizácie a algoritmy strojového učenia na hrane siete. Táto služba rozširuje možnosti AWS na hranu siete, aby sa lokálne dáta mohli spracúvať skôr a cloud sa mohol používať na správu alebo dodatočnú analýzu a trvalé ukladanie agregovaných dát. Inými slovami je to konkurent Microsoft Azure IoT Edge. Na obr. 3 môžete vidieť príklad takéhoto využitia AWS IoT Greengrass.

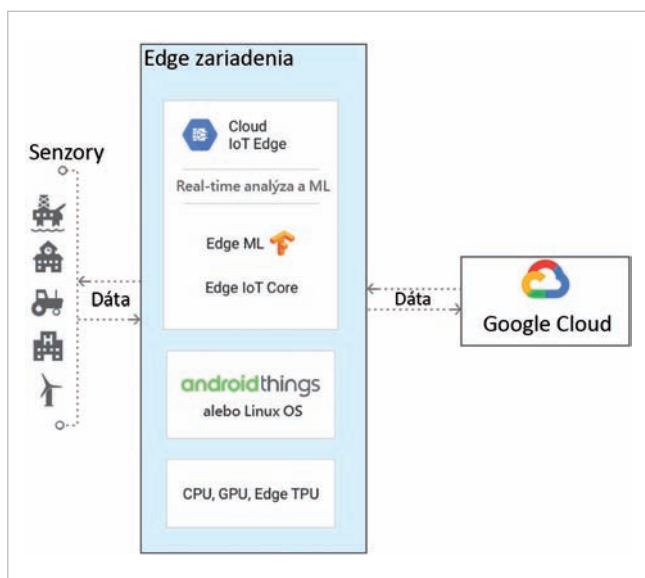
Tak ako pri Microsofte, aj tu môžu byť spustené služby na hrane siete, ktoré sú pri AWS typicke pre cloud. Takouto službou je napríklad AWS Lambda, ktorej úlohou sú spracovanie dát a ich preposielanie iným službám (computing). Pripojenie zariadení má na starosti služba AWS IoT Greengrass Connectors, strojové učenie zabezpečuje AWS IoT Greengrass ML Inference. AWS IoT Greengrass Core potrebuje na svoj chod ARM procesor s linuxovým jadrom. V tomto prípade neplatíte za jednotlivé služby, ale iba za AWS IoT Greengrass ako celok, kde sa ceny odvíjajú od množstva pripojených zariadení.



Obr. 3 AWS IoT Greengrass [7]

Google Cloud Platform

Google ponúka priamo aj zariadenie na edge computing s názvom Edge TPU a softvérový balík Cloud IoT Edge, ktorý poskytuje možnosti umelej inteligencie a strojového učenia pre inteligentné brány aj IoT zariadenia. To umožňuje vytvárať a trénovať modely strojového učenia na cloude a potom ich spúšťať priamo v Cloud IoT Edge prostredníctvom Edge TPU. Spomínané zariadenie už obsahuje aj koprocesor na strojové učenie. Cloud IoT Edge môže bežať aj na iných zariadeniach s operačnými systémami Android alebo Linux s procesormi ARM. Cloud IoT Edge môže obsahovať služby ako Edge ML na strojové učenie alebo Edge IoT Core na zber a odosielanie dát (obr. 4). Cenová politika je založená na množstve prenesených dát.



Obr. 4 Google Cloud IoT Edge [8]

IBM Cloud

Spoločnosť IBM ponúka platformu Watson IoT Platform Edge na automatizované nasadenie výpočtovej sily a služieb na hrane siete, čo umožňuje jednoduchú správu veľkých infraštruktúr uzlov na hrane siete a údržbu s aktualizáciou softvéru uzlov na hrane siete. Watson IoT Platform Edge umožňuje nasadenie IBM služieb, ale aj služieb tretích strán. Názov základnej služby pre edge computing je IoT Core Edge, ktorá ponúka lokálny MQTT broker na zber a odosielanie dát. Tento broker umožňuje komunikáciu medzi edge zariadeniami a cloudom a spravuje ukladanie a preposielanie dát. Služba navyše zabezpečuje filtráciu dát na hrane siete.

Aj v tomto prípade je táto platforma závislá od Dockeru s kontajnermi, kde má každá služba svoj vlastný kontajner. Uzly na hrane siete sa môžu značne líšiť veľkosťou. Nakoľko aj táto architektúra je založená na Dockery, aj v tomto prípade je potrebný operačný systém s linuxovým jadrom a procesorom ARM. Tu sa objavila aj minimálna požiadavka na operačnú pamäť, ktorá by mala mať minimálne 256 MB [9].

Táto služba je zatiaľ iba v testovacej fáze, a preto možnosti jej základnej architektúry v článku zatiaľ neuvádzame.

Záver

V tejto časti sme sa venovali najväčším poskytovateľom platformiem cloud a edge, pričom sme poukázali na možnosť nasadenia edge computingu aj bez potreby znalosti programovania. Každá spomínaná edge služba je navrhnutá tak, aby jednoducho komunikovala s cloudovou službou svojho poskytovateľa, ale nakoľko podporujú na komunikáciu tie isté protokoly (MQTT, AMQP, HTTP a HTTPS), nie je problém pripojiť ich aj ku konkurenčným cloudovým poskytovateľom; cenová politika je všade nastavená tak, aby sa také niečo neoplatilo. Existuje mnoho ďalších poskytovateľov edge platformi, ale v tomto článku sme sa zamerali len na najväčších z nich. V nasledujúcej časti seriálu sa budeme venovať nami realizovanými prípadovými štúdiami využívajúcimi výpočty na hrane siete.

Podakovanie

Publikácia bola podporená projektom KEGA 033TUKE-4/2018 AICyBS – Smart Industry/Architektúry inteligentných informačných a kybernetických systémov.

Referencie

- [1] Papcun, P. – Kajáti, E. – Vaščák, J. (2019). Smart/Intelligent edge – hardvérové parametre zariadení na hrane siete. In: ATP Journal, roč. 26, č. 6, s. 40 – 41. ISSN 1335-2237.
- [2] Papcun, P. – Kajáti, E. – Čupková, D. – Mocnej, J. – Miškuf, M. – Zolotová, I. (2019). Edge-enabled IoT gateway criteria selection and evaluation. [online]. In: Concurrency and Computation: Practice and Experience. Dostupné na: <https://doi.org/10.1002/cpe.5219>. (v tlači)
- [3] Kajáti, E. – Papcun, P. – Čupková, D. – Zolotová, I. (2019). Smart/Intelligent edge – kritériá výberu a hodnotenia parametrov riešení na hrane siete. In: ATP Journal, roč. 26, č. 5, s. 62 – 63. ISSN 1335-2237.
- [4] Čupková, D. – Kajáti, E. – Vaščák, J. – Papcun, P. (2019). Smart/Intelligent edge – umelá inteligencia v dátovej analytike na hrane siete. In: ATP Journal, roč. 26, č. 3, s. 54 – 55. ISSN 1335-2237.
- [5] Synergy resource group (2019). Cloud Infrastructure Services – Market Share. [online]. Citované 13. 5. 2019. Dostupné na: <https://techblog.comsoc.org/2019/02/05/synergy-research-cloud-service-provider-rankings/>.
- [6] Gremban, K. – Microsoft (2019). What is Azure IoT Edge. [online]. Citované 18. 5. 2019. Dostupné na: <https://docs.microsoft.com/en-us/azure/iot-edge/about-iot-edge>.
- [7] Baldacchino, S. – Rec, C. – Barr, J. – Amazon Web Services (2018). AWS IoT Greengrass. [online]. Citované 16. 5. 2019. Dostupné na: <https://aws.amazon.com/greengrass/>.
- [8] Rhee, I. – Google Cloud (2018). Bringing intelligence to the edge with Cloud IoT. [online]. Citované 25. 5. 2019. Dostupné na: <https://cloud.google.com/blog/products/gcp/bringing-intelligence-edge-cloud-iot>.
- [9] Kufluk, B. – IBM Developer (2018). Edge Technical Preview Now Available. [online]. Citované 20. 5. 2019. Dostupné na: <https://developer.ibm.com/iotplatform/2018/03/28/edge-technical-preview-now-available/>.

Ing. Peter Papcun, PhD.

Ing. Erik Kajáti

Ing. Dominika Čupková

prof. Ing. Iveta Zolotová, CSc.

Technická univerzita v Košiciach, FEI
Katedra kybernetiky a umelej inteligencie
Centrum inteligentných kybernetických systémov
<http://ics.fei.tuke.sk>

Nasleduj Alberta

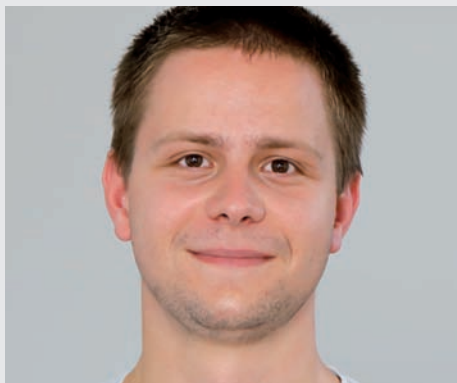
Zvedavosť je spoločným menovateľom mladých ľudí – študentov stredných odborných škôl a univerzít, ktorých vám v našej rubrike „Nasleduj Alberta“ budeme postupne predstavovať. Spája ich jedno – dokázali vyniknúť, pretože využili svoju zvedavosť po objavovaní. Vďaka svojim rodičom, pedagógom a nesporne z veľkej časti vlastnou disciplínou a zariadeniu majú „našliapnuté“ byť lídrami v tom, čo robia.



„NEMÁM ŽIADNY ZVLÁŠTNY TALENT. SOM IBA VÁŠNIVO ZVEDAVÝ.“

ALBERT EINSTEIN

Adam Trizuljak



... je v súčasnosti študentom druhého ročníka inžinierskeho štúdia v študijnom odbore robotika a kybernetika na FEI STU v Bratislave. V rokoch 2015 – 2016 absolvoval stáž v Nemeckej agentúre pre vesmír a letectvo (DLR) v Centre robotiky a mechatroniky, kde sa venoval vývoju roja miniatúrnych quadrokoptér. Už počas štúdia pracoval v spoločnosti Photoneo, ktorá vyvíja inovatívne priemyselné 3D laserové skenery a robotické bin-picking aplikácie. Bol ocenený ako Študent roka 2018 v kategórii najlepší študent druhého stupňa štúdia na FEI STU. V súčasnosti je na stáži v americkej firme Skydio v San Franciscu, ktorá vyvíja plne autonómne drony na filmovanie športových aktivít.

Ako si sa dostal k oblasti/odboru, ktorý v súčasnosti študuješ?

Od malička ma zaujímala elektronika a ako fungujú rôzne zariadenia. Na krúžkoch robotiky som sa dostal k programovaniu, vďaka čomu som sa rozhodol ísť študovať aplikovanú informatiku na FEI STU. Postupom času som však zistil, že ma viac baví pracovať s hardvérom a s vecami, čo sa hýbu, vnímajú prostredie a vedia s ním interagovať. Robotika ma priťahuje aj preto, lebo vyžaduje spájanie znalostí zo softvérového inžinierstva, elektrotechniky, mechatroniky a ďalších disciplín.

Čo ťa viedlo k tomu, že si sa začal zapájať do odborných aktivít aj vo svojom voľnom čase?

Už od detstva ma to ťahalo k technike všetkého druhu, preto som navštevoval rôzne krúžky elektrotechniky a robotiky a zapájal sa do súťaží ako Istrobot a RoboCup Jr. Počas štúdia na VŠ to potom bola hlavne potreba nájsť si zaujímavú prácu, aby som mohol získavať relevantnú prax v odbore, čo ma priviedlo do firmy Photoneo. V rámci štúdia som sa zapojil aj do aktivít v rámci Národného centra robotiky na FEI STU vedeného prof. Františkom Duchoňom. A keď sa mi naskytla možnosť absolvovať stáž v DLR, prirodzene som neváhal ju využiť.

Máš nejaký vzor (človeka, firmu...), ktorý ťa motivuje napredovať v tom, čo robíš/študuješ? Prečo práve on, resp. táto firma?

Najväčší vzor pre mňa predstavuje Teodor Tomić, PhD., aktuálne doktorand na Munich School of Robotics and Machine Intelligence, ktorý bol môj vedúci práce počas stáže v DLR a momentálne s ním pracujem vo firme Skydio. Obdivujem jeho znalosti v oblasti robotiky, jeho odbornú úroveň a cit pre vedeckú metódu, a k tomu má skvelú priateľskú povahu. Práve vďaka nemu som sa rozhodol ďalej pokračovať v štúdiu robotiky, dá sa povedať, že mi ukázal cestu.

Keby si mal spomenúť dve veci v oblasti techniky, ktoré by bolo podľa teba potrebné zásadne zmeniť/inovovať/vyvinúť, čo by to bolo? Ako by si to urobil ty?

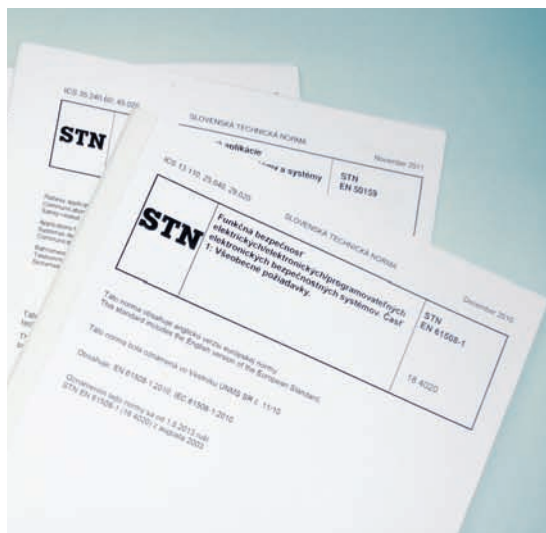
Určite musíme pracovať na prechode od fosílnych palív k čistým zdrojom energie. To je v súčasnosti predovšetkým solárna a veterná energia, ktorá však stále musí byť dopĺňaná vodnou a jadrovou energiou. Celkovo si myslím, že jadrová energetika je v súčasnosti našou najlepšou možnou voľbou, ale vzhľadom na to, ako citlivo je vnímaná, dúfam, že sa ju raz podarí nahradiť napríklad fúznou energiou. No a taký teleport a stroj času by tiež neboli na škodu.

Máš nejaký cieľ/métu, kam by si sa chcel vo svojom živote dopracovať (osobne, kariérne...)? Čo by si potreboval na dosiahnutie tohto cieľa?

Mojím aktuálnym cieľom je dokončiť a obhájiť moju diplomovú prácu. Nemám ešte úplne jasnú predstavu o tom, kam sa chcem kariérne dopracovať. Viem, že ma to ťahá smerom k výskumu, preto zvažujem pokračovať v PhD. štúdiu, je to však pre mňa zatiaľ otvorená otázka. Myslím si však, že by to bolo užitočné za každých okolností, či už skončím v komerčnej alebo akademickej sfére.

Akou krajinou by malo byť Slovensko, aby bolo pre teba príťažlivé zostať tu pracovať?

Máme silný automobilový priemysel, ktorý je však zameraný predovšetkým na montáž, pričom výskum a vývoj prebiehajú inde. S narastajúcou mierou automatizácie sa musíme snažiť orientovať viac na výskum, inak nám hrozí, že dopadneme ako Detroit. Je nutné pozdvihnúť úroveň nášho školstva a vedy, v prvom rade lepším financovaním, aby tu mohli vzniknúť výskumné centrá svetového významu a aby si univerzity dokázali udržať aj prilákať tých najkvalitnejších ľudí. Štát zároveň musí zabezpečiť priaznivé podnikateľské prostredie, stabilnú politickú situáciu a rozvoj spolupráce v rámci EÚ.



ELEKTROTECHNICKÉ STN

Prehľad vydaných elektrotechnických STN
a ich zmien (triedy 33, 34, 36, 92).

STN 92 0205/Z1: 2019-05 (92 0205) Správanie sa stavebných výrobkov a konštrukcií v požiari. Zachovanie funkčnej odolnosti káblových systémov. Požiadavky, skúšky, klasifikácia a aplikácia výsledkov skúšok.

STN EN 13501-1: 2019-05 (92 0850) Klasifikácia požiarnych charakteristík stavebných výrobkov a prvkov stavieb. Časť 1: Klasifikácia využívajúca údaje zo skúšok reakcie na oheň.*)

STN EN 13501-6: 2019-05 (92 0850) Klasifikácia požiarnych charakteristík stavebných výrobkov a prvkov stavieb. Časť 6: Klasifikácia využívajúca údaje zo skúšok reakcie silnoprúdových káblov, riadiacich káblov a komunikačných káblov.*)

STN EN 16925: 2019-05 (92 0421) Stabilné hasiace zariadenia. Sprinklerové systémy na použitie v budovách na bývanie. Projektovanie, inštalovanie a údržba.*)

STN P CEN/TS 54-14: 2019-05 (92 0404) Elektrická požiarňa signalizácia. Časť 14: Pokyny na navrhovanie, projektovanie, inštalovanie, uvedenie do prevádzky, prevádzkovanie a údržbu.*)

STN 33 2000-7-704: 2019-06 (33 2000) Elektrické inštalácie nízkeho napätia. Časť 7-704: Požiadavky na osobitné inštalácie alebo priestory. Inštalácie na staveniskách a búraniskách.

STN 33 2000-7-708: 2019-06 (33 2000) Elektrické inštalácie nízkeho napätia. Časť 7-708: Požiadavky na osobitné inštalácie alebo priestory. Karavanové parky, kempingy a podobné priestory.

STN EN 55016-4-2/A2/AC: 2019-06 (33 4216) Špecifikácia metód a meracích prístrojov na meranie rádiového rušenia a odolnosti proti nemu. Časť 4-2: Neistoty meraní, štatistiky a modelovanie medzí. Neistota meracích prístrojov.*)

STN EN IEC 60204-11: 2019-06 (33 2200) Bezpečnosť strojových zariadení. Elektrické zariadenia strojov. Časť 11: Požiadavky na zariadenia na striedavé napätie nad 1 000 V alebo na jednosmerné napätie nad 1 500 V a neprevyšujúce 36 kV.*)

STN EN IEC 61000-3-2: 2019-06 (33 3432) Elektromagnetická kompatibilita (EMC). Časť 3-2: Medze. Medze vyžarovania harmonických zložiek prúdu (zariadenia so vstupným fázovým prúdom ≤ 16 A).*)

STN EN IEC 61000-6-1: 2019-06 (33 3432) Elektromagnetická kompatibilita (EMC). Časť 6-1: Všeobecné normy. Norma na odolnosť pre prostredia obytné, obchodné a ľahkého priemyslu.*)

STN EN IEC 61000-6-2: 2019-06 (33 3432) Elektromagnetická kompatibilita (EMC). Časť 6-2: Všeobecné normy. Norma na odolnosť pre priemyselné prostredia.*)

STN EN IEC 61496-3: 2019-06 (33 2205) Bezpečnosť strojových zariadení. Elektrosenzitívne ochranné zariadenia. Časť 3: Osobitné požiadavky na aktívne optoelektronické ochranné zariadenia citlivé na rozptyľové odrazy (AOPDDR).*)

STN EN IEC 62474: 2019-06 (34 5904) Uvádzanie materiálov pri výrobkoch elektrotechnického priemyslu a pre elektrotechnický priemysel.*)

STN EN 12193: 2019-06 (36 0071) Svetlo a osvetlenie. Osvetlenie športovísk.*)

STN EN 13032-2: 2019-06 (36 0401) Svetlo a osvetlenie. Meranie a vyhodnotenie fotometrických údajov svetelných zdrojov a svietidiel. Časť 2: Prezentácia údajov pre vnútorné a vonkajšie pracoviská.

STN EN 50600-4-2/A1: 2019-06 (36 7254) Informačná technika. Zariadenia a infraštruktúry výpočtových stredísk. Časť 4-2: Efektívnosť využitia energie.*)

STN EN 50600-4-3/A1: 2019-06 (36 7254) Informačná technika. Zariadenia a infraštruktúry výpočtových stredísk. Časť 4-3: Činiteľ obnoviteľnosti energie.*)

STN EN 61010-1/A1: 2019-06 (36 2000) Bezpečnostné požiadavky na elektrické zariadenia na meranie, riadenie a laboratórne použitie. Časť 1: Všeobecné požiadavky.*)

STN EN IEC 60730-2-14: 2019-06 (36 1950) Automatické elektrické riadiace zariadenia. Časť 2-14: Osobitné požiadavky na elektrické ovládače.*)

STN EN IEC 60730-2-9: 2019-06 (36 1950) Automatické elektrické riadiace zariadenia. Časť 2-9: Osobitné požiadavky na riadiace zariadenia so snímaním teploty.*)

STN EN IEC 62087-7: 2019-06 (36 7004) Audio-, video- a podobné zariadenia. Určenie spotreby energie. Časť 7: Monitory počítačov.*)

STN EN IEC 63033-2: 2019-06 (36 8001) Multimediálne systémy a zariadenia automobilov. Systém na monitorovanie jazdy. Časť 2: Metódy záznamu systému na monitorovanie jazdy.*)

STN P CEN ISO/TS 21805: 2019-06 (92 0433) Pokyny na navrhovanie, výber a inštalovanie vetracích otvorov na ochranu konštrukčnej celistvosti uzatvorených priestorov chránených plynovými hasiacimi zariadeniami (ISO/TS 21805: 2018).*)

*Mesiac vydania STN je uvedený
za jej označením v tvare „: 2019-06“.*

**) Normy boli vydané v anglickom jazyku.*

Ing. Ludovít Harnoš
viceprezident SEZ-KES

www.sez-kes.sk

Distributed Applications and Interoperable Systems

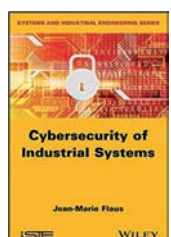
Autori: Pereira, J. – Ricci, L., rok vydania: 2019,
vydavateľ: Springer, ISBN 978-3-030-22496-7 (e-Book),
publikáciu možno zakúpiť na www.springer.com.



Ide o zborník z 19. medzinárodnej konferencie IFIP o distribuovaných aplikáciách a vzájomne spolupracujúcich a prepojených systémoch, DAIS 2019, ktorá sa konala v Kongens Lyngby v Dánsku v júni 2019 v rámci 14. medzinárodnej federatívnej konferencie o distribuovaných výpočtových technikách DisCoTec 2019. Do tejto publikácie bolo vybraných a starostlivo zrecenzovaných deväť kompletných referátov spolu s dvomi krátkymi dokumentmi z celkovo 28 prihlásených príspevkov. Príspevky riešili výzvy vo viacerých aplikačných oblastiach, ako je napríklad internet vecí, cloudové výpočty či mobilné systémy. Niektoré dokumenty sa zameriavali na middleware na riadenie súbežnosti a konzistentnosti v distribuovaných systémoch vrátane replikácie údajov a transakcií.

Cybersecurity of Industrial Systems

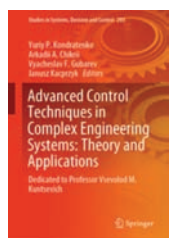
Autor: Flaus, J.-M., rok vydania: 2019,
vydavateľstvo: Wiley-ISTE, ISBN 978-1-78630421-6,
publikáciu možno zakúpiť na www.amazon.com.



Riadenie kybernetickej bezpečnosti priemyselných systémov je kľúčovou otázkou. Na implementáciu príslušných riešení musí mať manažér priemyselnej prevádzky jasnú predstavu o informačných systémoch, komunikačných sieťach a riadiacich a bezpečnostných systémoch. Musí mať tiež určité vedomosti o metódach, ktoré útočníci používajú, o príslušných normách a predpisoch a o dostupných riešeniach bezpečnosti. Táto publikácia prezentuje tieto témy s cieľom poskytnúť podrobný prehľad a pomôcť čitateľovi riešiť správu kybernetickej bezpečnosti a jej inštalácie. Kniha sa zaoberá týmito otázkami v rámci klasických systémov architektúry SCADA a systémov priemyselného internetu vecí (IIoT).

Advanced Control Techniques in Complex Engineering Systems: Theory and Applications

Autori: Kondratenko, Y. P. – Chikrii, A. A. – Gubarev, V. F. – Kacprzyk, J., rok vydania: 2019,
vydavateľstvo: Springer, ISBN 978-3-030-21926-0,
publikáciu možno zakúpiť na www.springer.com.



Uvedená publikácia predstavuje autoritativnú zbierku príspevkov výskumníkov zo 16 rôznych krajín, ktoré informujú o najnovšom vývoji a nových smeroch v pokročilých systémoch riadenia, ako aj o nových teoretických poznatkoch, priemyselných aplikáciách a prípadových štúdiách komplexných technických systémov. Táto kniha je venovaná profesorovi Vsevolodovi Michailovičovi Kunčevičovi, akademikovi Národnej akadémie vied Ukrajiny a predsedovi Národného výboru ukrajinskej asociácie pre automatizáciu, ako uznanie za jeho priekopnícke diela, veľké vedecké a výskumné úspechy a dlhoročné služby v mnohých vedeckých a odborných komunitách, najmä tých, ktoré sa zaoberajú automatizáciou, kybernetikou, riadením a konkrétnejšie základmi

a aplikáciami nástrojov a techník na riešenie neistých informácií, odolnosti, nelinearity, extrémnych systémov, diskretných a adaptívnych riadiacich systémov a pod. Kniha ponúka základné teórie, metódy a nové výzvy v návrhoch riadiacich systémov. Nie je len aktuálnym referenčným sprievodcom, ale aj zdrojom nových nápadov a inšpirácií pre študentov a výskumných pracovníkov. Jej 15 kapitol je rozdelených do štyroch častí: (a) základné teoretické otázky týkajúce sa zložitých technických systémov, (b) umelá inteligencia a soft computing pre systémy riadenia a rozhodovania, (c) pokročilé riadiace techniky pre priemyselnú a kolaboratívnu automatizáciu a (d) moderné aplikácie na riadenie a spracovanie informácií v komplexných systémoch. Všetky kapitoly majú poskytnúť jednoduchý úvod k riešeným témam vrátane najdôležitejších referencií. Zároveň odzrkadľujú rôzne aspekty najnovšej výskumnej práce, ktorá sa vykonáva na celom svete, a preto poskytujú informácie o stave techniky.

Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing (Springer Series in Advanced Manufacturing). 1st ed.

Autori: Thames, L. – Schaefer, D., rok vydania: 2017,
vydavateľstvo: Springer, ISBN 978-3-319-50659-3,
publikáciu možno zakúpiť na www.springer.com.



Publikácia predstavuje čitateľom kybernetickú bezpečnosť a jej vplyv na realizáciu vízie Priemyslu 4.0. Uvádza technologické základy kybernetickej bezpečnosti v rámci priestoru Priemyslu 4.0 a podrobne opisuje existujúce hrozby, ktorým čelí Priemysel 4.0, ako aj najmodernejšie riešenia, pokiaľ ide o akademický výskum a praktické implementácie. Opísané sú Priemysel 4.0 a jeho pridružené technológie, ako je priemyselný internet vecí, riešenia využívajúce cloudové technológie a výrobné systémy vrátane súvisiacich prelomových inovácií. Kniha je hodnotný zdroj pre praktických technikov a ľudí s rozhodovacou právomocou v priemysle, ako aj pre výskumných pracovníkov v projekčných a výrobných komunitách a všetkých záujemcov o Priemysel 4.0 a kybernetickú bezpečnosť.

Artificial Intelligence Applications and Innovations

Autor: MacIntyre, J. – Maglogiannis, I. – Iliadis, L. – Pimenidis, E., rok vydania: 2019, vydavateľstvo: Springer, ISBN 978-3-030-19822-0,
publikáciu možno zakúpiť na www.springer.com.



Kniha obsahuje príspevky z 15. medzinárodnej konferencie IFIP WG 12.5 o aplikáciách a inováciách umelej inteligencie, AIAI 2019, ktorá sa konala v máji 2019 v Hersonissose na Kréte v Grécku. Z celkového počtu 101 príspevkov bolo vybratých 49 kompletných referátov a šesť prezentovaných krátkych referátov. Zahŕňajú širokú škálu tém, ako je hlbkové učenie ANN, genetické algoritmy – optimalizácia, modelovanie obmedzení, tréningové algoritmy ANN, inteligentné modelovanie sociálnych médií, ťažba textov/strojový preklad, fuzzy modelovanie, biomedicínske a bioinformatické algoritmy a systémy a mnohé iné.

Hlavní partneri



B+R automatizace, spol. s r.o.
– organizačná zložka
www.br-automation.com



AutoCont Control spol. s r.o.
www.autocontcontrol.sk

SIEMENS

Siemens s.r.o.
www.siemens.sk

V celoročnej súťaži môžete vyhrať tieto hlavné ceny:



Elektrická kolobežka
Eljet Carbon light black



Digitálny fotoaparát
Canon EOS 4000D



Automatický kávovar
SIEMENS TI30A209RW

ČITATEĽSKÁ SÚŤAŽ ATP JOURNAL 7/2019

Partneri kola súťaže:



Phoenix Contact, s.r.o.



Universal Robots A/S



ABB, s.r.o.

V tomto kole súťažíte o tieto vecné ceny:



Kliešte, orezávač, dáždnik



Termoska, model robota



Slúchadlá

Otázky sú veľmi jednoduché. Ak by ste predsa len nepoznali odpovede, pretože vašou parketou je iná oblasť, môžete ich nájsť v tomto čísle ATP Journal, ako aj v článkoch uverejnených na stránke www.atpjournall.sk.

Súťažné otázky:

1. Pomocou akého SW je možné rýchlo naprogramovať logický reléový systém PLC logic?
2. Na akú operáciu je primárne určený kolaboratívny robot UR10 nasadený v spoločnosti 2D & S, s.r.o.?
3. Ktoré štyri oblasti pokrýva proces merania robustnosti a integrity bezpečnosti v rámci nezávislého centra zabezpečenia zariadení (DSAC) spoločnosti ABB?
4. A teraz jedna prázdninová otázka, na ktorú nemusíte hľadať odpoveď. Prečo (okrem možnosti súťažiť 😊) odoberáte ATP Journal?

Súťažte prostredníctvom www.atpjournall.sk/sutaz/otazky

Odpovede posielajte najneskôr do 15. 8. 2019

Pravidlá súťaže sú uverejnené v ATP Journal 1/2019 na str. 55 a na www.atpjournall.sk/sutaz

ČITATEĽSKÁ SÚŤAŽ

ATP JOURNAL 5/2019

VYHODNOTENIE

Správne odpovede

- 1. Čo dokáže päťprstová ruka SCHUNK SVH vďaka umelej inteligencii?**
Identifikovať ľubovoľné objekty v ľubovoľnej polohe a autonómne vyvíjať a realizovať príslušné stratégie uchopovania.
- 2. Aké komponenty sú súčasťou strojového videnia od B&R?**
Kamera, riadenie stroboskopu a svetlá.
- 3. Vďaka čomu možno pripojiť čítaciu hlavu Q300 aj v HF projektoch?**
Vďaka externým anténam pripojiteľným priamo na hlavu UHF.
- 4. Ako sa volá konferencia, ktorej druhý ročník spoločne zorganizovali redakcie ATP Journal a ai magazine?**
Robotika vo výrobnej praxi malých a stredných podnikov.

Výhercovia

Pavol Kubiš, Hniezdne

Peter Vojtech, Veľké Bierovce

Roman Michalík, Martin

Srdečne gratulujeme.

Bezplatný odber

www.atpjournalsk/registracia

tlačenej alebo digitálnej verzie

ZOZNAM FIRIEM PUBLIKUJÚCICH V TOMTO ČÍSLE

Firma • Strana (o – obálka)

ABB, s.r.o. • 22 – 23

Beckhoff Česká republika s.r.o. • o4, 28 – 29

B+R automatizace, spol. s r.o. – organizačná zložka • o1

ControlSystem, s.r.o. • 38

D-Ex Instruments, s.r.o. • 33

EPLAN ENGINEERING CZ, s.r.o. – organizačná zložka • 18

EWWH, s.r.o. • 24

FANUC Slovakia s.r.o. • 31

KALIBRÁTORY, s.r.o. • 37

MARPEX s.r.o. • 8 – 11, 12 – 14

Murrelektronik Slovakia s.r.o. • 39

OBO BETTERMANN s.r.o. • 19

ProCS, s.r.o. • 20 – 21

PHOENIX CONTACT, s.r.o. • 25

PREMIER FARNELL UK Ltd. • 29, 40 – 41

SIEMENS, s.r.o. • o3, 26 – 27

Slovenská elektrizačná prenosová sústava, a. s. • 1

Universal Robots A/S • o2, 16 – 17

YASKAWA Czech s.r.o. • 32

Redakčná rada

prof. Ing. Alexík Mikuláš, PhD., FRI ŽU, Žilina
Ing. Balogh Richard, PhD., FEI STU, Bratislava
prof. Ing. Belavý Cyril, CSc., SJF STU, Bratislava
prof. Ing. Duchoň František, PhD., FEI STU – NCR, Bratislava
prof. Ing. Fikar Miroslav, DrSc., FCHPT STU, Bratislava
prof. Ing. Huličák Gabriel, DrSc., SJF STU, Bratislava
prof. Ing. Janíček František, PhD., FEI STU, Bratislava
prof. Ing. Krokavec Dušan, CSc., FEI TU Košice
doc. Ing. Kvasnica Michal, PhD., FCHPT STU, Bratislava
prof. Ing. Malindžák Dušan, CSc., BERG TU, Košice
prof. Ing. Mészáros Alajos, CSc., FCHPT STU, Bratislava
prof. Ing. Murgáš Ján, PhD., FEI STU, Bratislava
prof. Ing. Rástočný Karol, PhD., FEIT ŽU, Žilina
doc. Ing. Schreiber Peter, CSc., MTF STU, Trnava
prof. Ing. Smieško Viktor, PhD., FEI STU, Bratislava
prof. Ing. Taufer Ivan, DrSc., FEI Univerzita Pardubice
prof. Ing. Veselý Vojtech, DrSc., FEI STU, Bratislava
prof. Ing. Zolotová Iveta, CSc., FEI TU, Košice
prof. Ing. Žalman Milan, PhD., FEI STU, Bratislava
doc. Ing. Ždánsky Juraj, PhD., FEIT ŽU, Žilina

Babic Branislav,
výkonný riaditeľ ProCS, s.r.o.

Ing. Horváth Tomáš,
riaditeľ HMH, s.r.o.

Ing. Hrica Marián,
riaditeľ divízie A & D, Siemens, s.r.o.

Kroupa Jiří,
riaditeľ kancelárie pre SK, DEHN+SOHN

Ing. Lásik Vladimír,
PPA CONTROLL, a.s.

Ing. Mašláni Marek,
riaditeľ B+R automatizace, s.r.o. – o. z.

Mík Pavel,
obchodný riaditeľ ABB, s.r.o.

Ing. Petergáč Štefan,
predseda predstavenstva Datalan, a.s.

Ing. Széplaky Ladislav,
riaditeľ Emerson Process Management, s.r.o.

Redakcia

ATP Journal
Galvaniho 7/D
821 04 Bratislava
tel.: +421 2 32 332 182
fax: +421 2 32 332 109
vydavatelstvo@hmh.sk
www.atpjournalsk

Ing. Anton Géner, šéfredaktor
gener@hmh.sk

Zuzana Pettingerová, DTP grafik
dtp@hmh.sk

Dagmar Votavová, obchod a marketing
podklady@hmh.sk, mediamarketing@hmh.sk

Mgr. Bronislava Chocholová
jazyková redaktorka

Vydavateľstvo

HMH, s.r.o.
Tavariškova osada 39
841 02 Bratislava 42
IČO: 31356273

Vydavateľ periodickej tlače nemá hlasovacie práva
alebo podiely na základnom imaní žiadneho vydávateľa.

Spoluzakladateľ

Katedra ASR, EF STU
Katedra automatizácie a regulácie, EF STU
Katedra automatizácie, ChtF STU
PPA CONTROLL, a.s.

Zaregistrované MK SR pod číslom EV 3242/09 & Vychádza mesačne & Cena pre registrovaných čitateľov 0 € & Cena jedného výtlačku vo voľnom predaji: 3,30 € + DPH & Objednávky na ATP Journal vybavuje redakcia na svojej adrese & Tlač a knižárske spracovanie KASICO a.s. & Redakcia nezodpovedá za správnosť inzerátov a inzertných článkov & Nevyžiadané materiály nevraciame & Dátum vydania: júl 2019

ISSN 1335-2237 (tlačaná verzia)
ISSN 1336-233X (on-line verzia)

SIEMENS
Ingenuity for life



Digitalizácia pre váš podnik

www.siemens.sk/digitalizacia

Minimální rozměry a maximální možnosti.

Ultra-kompaktní průmyslový počítač C6015.



www.beckhoff.cz/C6015

Díky ultra-kompaktnímu průmyslovému PC C6015 společnost Beckhoff opět rozšiřuje možnosti aplikací s řízením na bázi IPC. Tato nová generace IPC nabízí vynikající poměr ceny a výkonu ve výjimečně kompaktním těle všude tam, kde bylo dříve použití PC řízení nemožné z důvodu omezeného prostoru nebo nákladů. S možností až čtyřjádrového procesoru, nízkou hmotností a velkou flexibilitou lze C6015 univerzálně použít pro úkoly řízení, vizualizace, sběru dat a komunikace. Je také ideální jako gateway IoT.

- Procesor: Intel® Atom™, 1, 2 nebo 4 jádra
- Rozhraní: 2 Ethernet, 1 DisplayPort, 2 USB
- Hlavní paměť: až 4 GB paměti DDR3L RAM
- Provedení těla: slitina hliníku a zinku
- Rozměry (Š x V x H): 82 x 82 x 40 mm



Flexibilní instalace na stěnu rozvaděče za zadní nebo boční stranu IPC.

New Automation Technology

BECKHOFF